N°114

COMPRENDRE, UTILISER & ADMINISTRER LINUX

GNU LINUX PRATIQUE

JUIL. AOÛT 2019

FRANCE MÉTRO. : 7,90 €
DOM/TOM : 8,50 €
BEL/LUX/PORT. CONT. : 8,90 €
CH : 13 CHF
CAN : 14 $CAD
MAR : 98 MAD
TUN : 20 TND

SÉCURITÉ
Sécurisez les données sensibles de votre infrastructure avec Ansible Vault p. 38

SYSTÈME
Réaliser une sauvegarde et la restaurer avec Btrfs p. 24

SERVEUR
Installer, configurer et sécuriser un serveur Apache2 p. 30

SCIENCES
Découvrez eLabFTW, un cahier de laboratoire en ligne et collaboratif p. 72

WIFI / SÉCURITÉ

CRÉEZ VOTRE HOTSPOT WIFI SÉCURISÉ
CHEZ VOUS OU EN ENTREPRISE
p. 46

L 18864 - 114 - F: 7,90 € - RD

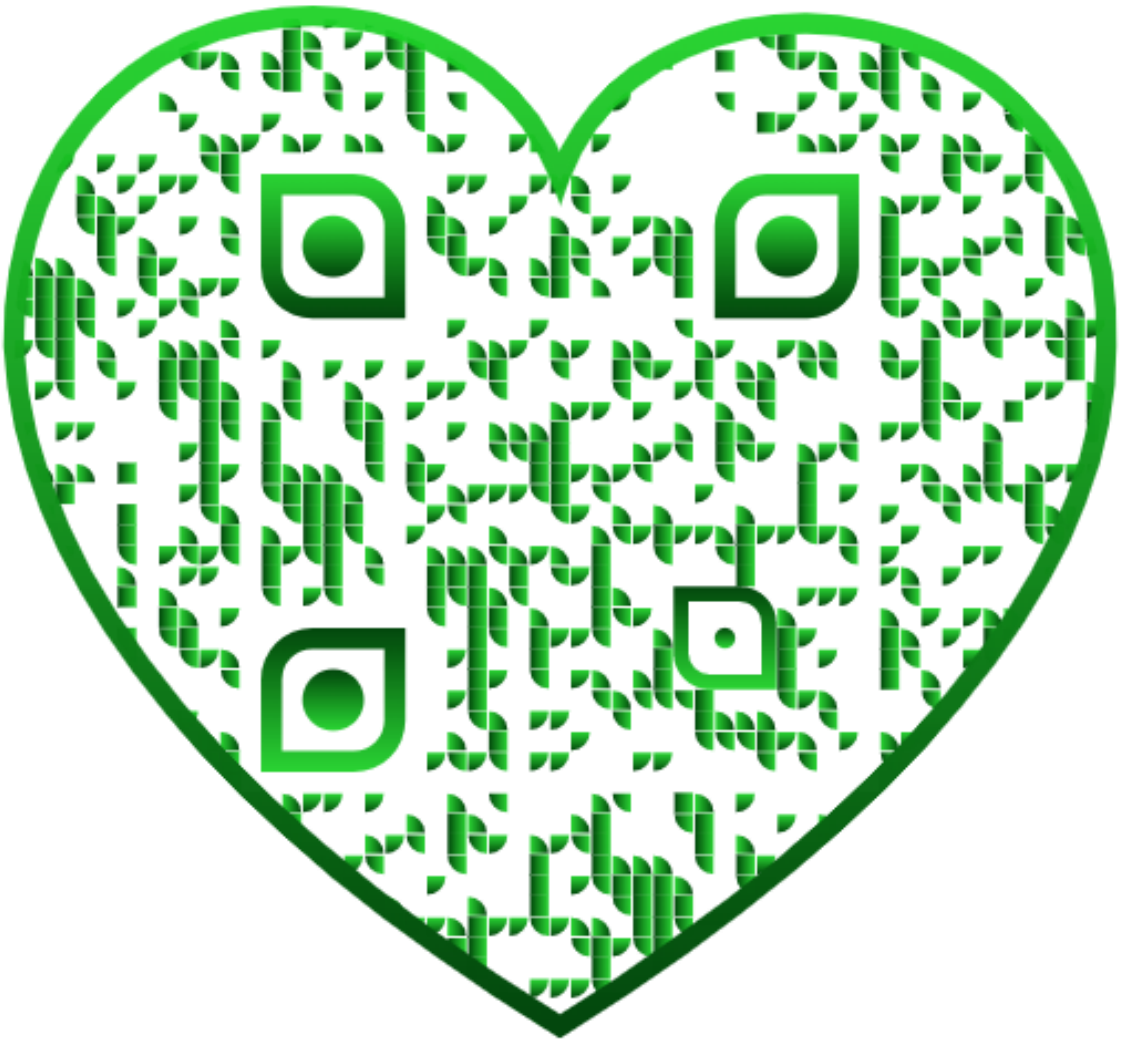
TUTORIELS

BUREAUTIQUE
Modifiez et créez vos propres polices à l'aide de FontForge p. 14

AUDIO
Réalisez vos enregistrements audio en toute simplicité avec Audio-Recorder p. 08

RED HAT / CENTOS
Bien configurer votre réseau et le dépanner avec les bons outils en cas de problème p. 62

ENTREPRISE
Le RGPD expliqué aux informaticiens p. 80



CSAW'19 EUROPE

20-29 SEPTEMBRE 2019

RED TEAM COMPETITION

csaw.io/red

COMPÉTITION DE CYBERSÉCURITÉ

RED TEAM : Repoussez vos limites !
Participez à la simulation d'infiltration
du système d'information d'une entreprise

- **Expérimentés** ou **débutants**, créez votre équipe !
- Qualifiez-vous en ligne du **20 au 29 septembre 2019**
- Participez à la finale sur le site de Valence le **7 novembre 2019**
  (frais de déplacement pris en charge selon le règlement du concours)
- Venez rencontrer des passionnés et des professionnels
- De nombreux lots à gagner !

---

red@esisar.grenoble-inp.fr @CsawEurope facebook/CSAWEsisar

GNU LINUX PRATIQUE

Grenoble INP ESISAR

GNU LINUX PRATIQUE EN NUMÉRIQUE ?

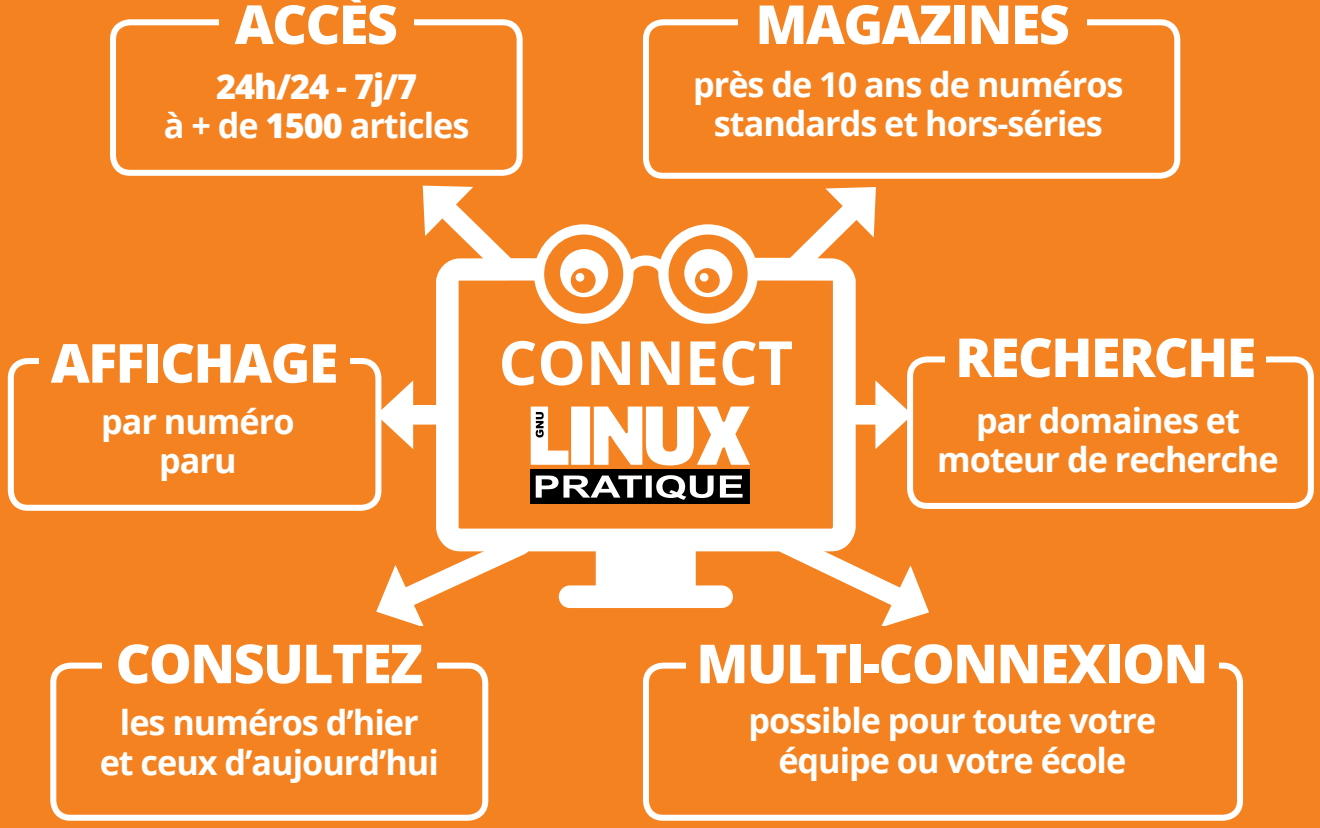
BIENVENUE SUR CONNECT !

CONNECT
LA PLATE-FORME DE LECTURE EN LIGNE DES ÉDITIONS DIAMOND
Identifiez vous
S'inscrire
Votre recherche
LINUX MAGAZINE FRANCE
MISC
LINUX PRATIQUE
HACKABLE MAGAZINE
A PROPOS
ABONNEZ-VOUS
Accueil » Linux Pratique
BIENVENUE SUR LA PLATEFORME DE DOCUMENTATION NUMÉRIQUE DE LINUX PRATIQUE !
CRÉEZ VOTRE HOTSPOT WIFI SÉCURISÉ
Linux Pratique n° 114
AUTHENTIFICATION DE L'ACCÈS À VOTRE RÉSEAU : MISE EN PLACE D'UN PORTAIL CAPTIF ET D'UN SERVICE 802.1X
Un portail captif est un élément de contrôle mandataire régulant l'accès au réseau pour les clients équipés d'un navigateur web. Dans cet article, nous allons voir comment intégrer cet élément dans une infrastructure pour authentifier les clients connectés en Wi-Fi avant leur accès effectif au réseau extérieur. Nous allons également présenter le 802.1X qui vise à authentifier les utilisateurs avant tout accès au réseau.
> Lire l'extrait
LES ARTICLES DE LINUX PRATIQUE N°114 - JUILLET/AOÛT 2019
Édito
Linux Pratique n° 114 | juillet 2019 | Aline Hof
Pour occuper votre été, nous avons choisi de vous concocter un nouveau numéro varié avec des sujets qui pourraient tout aussi bien vous être...
> Lire l'extrait
Brèves Linux Pratique Juillet/Août 2019
Linux Pratique n° 114 | juillet 2019 | Aline Hof
Libre à vous ! : l'émission radio de l'April / Mobilizon, un projet libre et fédéré pour organiser ses événements / Qwant Causes :...
> Lire l'extrait
Enregistrer le son avec Audio Recorder
Linux Pratique n° 114 | juillet 2019 | Anthony Carré
Pour enregistrer le son qui sort de vos enceintes, celui d'une application, d'une radio en streaming ou depuis un microphone, il existe un...
> Lire l'extrait
Worldwide Radio : les radios du monde entier en un tour de main
Linux Pratique n° 114 | juillet 2019 | Aline Hof
Disponible pour Firefox et Chrome/Chromium, Worldwide Radio vous permettra de profiter d'un large choix de stations radio à travers le monde en...
> Lire l'extrait
FoxClocks : Pour être à l'heure aux quatre coins de la planète
Linux Pratique n° 114 | juillet 2019 | Aline Hof
Utile si vous travaillez avec des collaborateurs aux quatre coins de la planète ou si vous avez de la famille ou des amis disséminés sur divers...
> Lire l'extrait
Modifiez et créez vos propres polices avec FontForge
Linux Pratique n° 114 | juillet 2019 | Yann Morère
Il existe des milliers de polices de caractères libres d'accès sur Internet. Cependant, certaines ne sont pas libres de droits ou encore ne...
> Lire l'extrait
RECHERCHER
UN ARTICLE LINUX PRATIQUE
parmi plus de 1550 articles !
Votre recherche
ACCÈS PAR NUMÉRO
NUMÉROS STANDARDS
114 113 112 111 110 109 108 107
106 105 104 103 102 101 100 099
098 097 096 095 094 093 092 091
>>
NUMÉROS HORS SÉRIE
045 044 043 042 041 040 039 038
037 036 035 034 033 032 031 030
029 028 027 026 025 024 023 022
>>
PAR DOMAINES
Brèves Bureautique Code Droit
Électronique Embarqué Graphisme Hacks
Humeur et Critique IA Mobilité Réseau
Sécurité Société Système Témoignage
Tests et prise en main Web

FACILITEZ-VOUS LA VEILLE TECHNO ET L'ACCÈS À LA DOCUMENTATION !

À découvrir sur :

connect.ed-diamond.com



Pour vous abonner :

www.ed-diamond.com

Pour un devis personnalisé ou pour en savoir plus :

Tél. : +33 (0)3 67 10 00 20 • E-mail : cial@ed-diamond.com

LINUX PRATIQUE est édité par
Les Éditions Diamond

10, Place de la Cathédrale - 68000 Colmar - France
Tél. : 03 67 10 00 20 | **Fax** : 03 67 10 00 21

E-mail : cial@ed-diamond.com
lecteurs@linux-pratique.com
Service commercial :
abo@linux-pratique.com
Sites : https://www.linux-pratique.com
https://www.ed-diamond.com

Directeur de publication : Arnaud Metzler
Chef des rédactions : Denis Bodor
Rédactrice en chef : Aline Hof
Responsable service infographie : Kathrin Scali
Responsable publicité : Tél. : 03 67 10 00 27
Service abonnement : Tél. : 03 67 10 00 20
Photographie et images : http://www.fotolia.com
Impression : pva, Landau, Allemagne
Distribution France :
(uniquement pour les dépositaires de presse)
MLP Réassort :
Plate-forme de Saint-Barthélemy-d'Anjou
Tél. : 02 41 27 53 12
Plate-forme de Saint-Quentin-Fallavier
Tél. : 04 74 82 63 04
Service des ventes :
Distri-médias : Tél. : 05 34 52 34 01

IMPRIMÉ en Allemagne - PRINTED in Germany

Dépôt légal : A parution
N° ISSN : 0183-0872
Commission Paritaire : K78 990
Périodicité : Bimestrielle
Prix de vente : 7,90 Euros

La rédaction n'est pas responsable des textes, illustrations et photos qui lui sont communiqués par leurs auteurs. La reproduction totale ou partielle des articles publiés dans Linux Pratique est interdite sans accord écrit de la société Les Éditions Diamond. Sauf accord particulier, les manuscrits, photos et dessins adressés à Linux Pratique, publiés ou non, ne sont ni rendus, ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire. Toutes les marques citées dans ce numéro sont déposées par leur propriétaire respectif. Tous les logos représentés dans le magazine sont la propriété de leur ayant droit respectif. Les articles non signés contenus dans ce numéro ont été rédigés par les membres de l'équipe rédactionnelle des Éditions Diamond.

LES ÉDITIONS DIAMOND
STIMULANT DE MATIÈRE GRISE

Membre April
www.april.org

Retrouvez-nous sur :

@linuxpratique
@editionsdiamond

@linuxpratique

https://connect.ed-diamond.com

https://www.linux-pratique.com
https://www.editions-diamond.fr

ENCART CONNECT ENCARTÉ DANS LA COUVERTURE

édito

Linux Pratique n°114

Pour occuper votre été, nous avons choisi de vous concocter un nouveau numéro varié avec des sujets qui pourraient tout aussi bien vous être utiles chez vous que sur votre lieu de travail…

Vous pourrez commencer par laisser libre cours à votre fibre artistique en créant votre propre police de caractères à l'aide de FontForge. Nous nous intéresserons aussi à Audio Recorder, un outil qui vous permettra de réaliser vos enregistrements sonores. Si vous avez un peu de temps devant vous, il sera peut-être l'occasion de vous pencher sur des tâches que vous remettez à plus tard comme la sauvegarde de vos données – on vous présentera ici la marche à suivre à l'aide de la fonctionnalité d'instantané de Btrfs – ou la sécurisation de vos secrets avec Ansible Vault – si vous avez apprécié l'article phare du précédent numéro, celui-ci vous offre une belle suite.

En parlant justement d'article phare, celui de ce numéro-ci vous guidera dans la création d'un hotspot wifi sécurisé. Que vous souhaitiez déployer une telle installation chez vous ou en entreprise, cet article détaillé vous expliquera comment mettre en place un portail captif à l'aide de la solution pfSense et comment utiliser un service 802.1X qui permettra d'authentifier vos utilisateurs avant tout accès au réseau.

L'été est peut-être aussi l'occasion rêvée de revoir quelques « basiques » avant la reprise en septembre : vous trouverez dans ce numéro un tutoriel qui vous accompagnera dans l'installation, la configuration et la sécurisation d'un serveur Apache 2. Nous ferons aussi le point sur un texte qui a fait beaucoup de bruit (et qui continue d'en faire) depuis son entrée en vigueur l'an passé : le Règlement Général sur la Protection des Données (RGPD pour les intimes).

Enfin, votre magazine vous promet comme à son habitude de belles découvertes et ce numéro-ci ne fait pas exception : vous pourrez partir à la rencontre du collectif associatif Low Tech Lab qui promeut l'utilisation de low-technologies, mais aussi découvrir le projet de cahier de laboratoire collaboratif eLabFTW.

Bel été et rendez-vous le 30 août prochain pour préparer ensemble la rentrée à l'occasion d'un nouveau numéro !

ALINE HOF

https://www.ed-diamond.com
OFFRES D'ABONNEMENTS | ANCIENS NUMÉROS | HORS-SÉRIES | DOCUMENTATION NUMÉRIQUE

Sommaire

Linux Pratique n°114

ACTUALITÉS & NOUVEAUTÉS

06 BRÈVES JUILLET - AOÛT 2019

LOGITHÈQUE & APPLICATIF

08 ENREGISTRER LE SON AVEC AUDIO RECORDER
Pour enregistrer le son qui sort de vos enceintes, celui d'une application, d'une radio en streaming ou depuis un microphone, il existe un grand nombre d'applications...

12 WORLDWIDE RADIO - LES RADIOS DU MONDE ENTIER EN UN TOUR DE MAIN

13 FOXCLOCKS - POUR ÊTRE À L'HEURE AUX QUATRE COINS DE LA PLANÈTE

14 MODIFIEZ ET CRÉEZ VOS PROPRES POLICES AVEC FONTFORGE
Il existe des milliers de polices de caractères libres d'accès sur Internet. Cependant, certaines ne sont pas libres de droits ou encore ne possèdent pas les caractères accentués et deviennent de fait inutilisables en langue française...

SYSTÈME & CONFIGURATION

24 RÉALISER UNE SAUVEGARDE ET LA RESTAURER AVEC BTRFS
Disponible depuis maintenant presque 10 ans, Btrfs est un système de fichiers mature qui est poussé par SUSE, il est devenu le système de fichiers par défaut lors de son installation...

RÉSEAU & ADMINISTRATION

30 INSTALLER, CONFIGURER ET SÉCURISER UN SERVEUR APACHE2
Apache est un serveur web : tout comme Tomcat et Nginx, il permet de servir des pages web aux internautes. Après l'avoir installé, nous découvrirons les principaux fichiers de configuration et commandes à connaître...

En couverture

46 Tout ce qu'il faut savoir pour mettre en place votre hotspot wifi sécurisé chez vous ou en entreprise

Système

24 Réaliser une sauvegarde et la restaurer avec la fonctionnalité d'instantané de Btrfs

Entreprise
RGPD
80
Le point sur le Règlement Général sur la Protection des Données et sur ce qu'il implique concrètement pour les informaticiens

38 SÉCURISEZ LES SECRETS DE VOTRE INFRASTRUCTURE AVEC ANSIBLE
Un précédent article a déjà présenté en détail le fonctionnement et l'utilisation de Ansible. Nous allons donc repartir de là et aller un peu plus loin en abordant la problématique, difficile et souvent complexe, de la gestion des secrets...

46 AUTHENTIFICATION DE L'ACCÈS À VOTRE RÉSEAU : MISE EN PLACE D'UN PORTAIL CAPTIF ET D'UN SERVICE 802.1X
Un portail captif est un élément de contrôle mandataire régulant l'accès au réseau pour les clients équipés d'un navigateur web. Dans cet article, nous allons voir comment intégrer cet élément dans une infrastructure...

62 OPTIMISER LES CONNEXIONS RÉSEAUX SOUS CENTOS/RHEL 7
Dans cet article, on aura l'occasion de plonger en profondeur dans la configuration réseau des machines sous CentOS 7 / RHEL 7...

MOBILITÉ & IOT

70 ANDROPEN OFFICE : RETROUVEZ UNE SUITE BUREAUTIQUE SUR MOBILE

71 PRIVATE BROWSER ET NAVIGATION INCOGNITO : UNE NAVIGATION PRIVÉE ET ANONYME

ENTREPRISE & ORGANISATION

72 ELABFTW, VOTRE CAHIER DE LABORATOIRE NUMÉRIQUE
L'ensemble des travaux scientifiques des chercheurs est retranscrit dans leurs cahiers de laboratoire afin de détailler les expériences, les théories, les conclusions...

80 LE RGPD EXPLIQUÉ AUX INFORMATICIENS
Entré en application le 25 mai 2018, le Règlement Général sur la Protection des Données est une avancée majeure pour la protection des données personnelles. Il est pourtant souvent perçu de différentes façons...

RÉFLEXION & SOCIÉTÉ

94 L'OPEN SOURCE AU CŒUR DU PARTAGE DE LOW-TECHNOLOGIES : À LA DÉCOUVERTE DU LOW TECH LAB
Marier open source, basses ou « low » technologies et développement durable, tel est l'un des objectifs suivis par le Low Tech Lab, un collectif associatif qui se veut promouvoir les solutions utiles et durables...

» 57 ABONNEMENTS

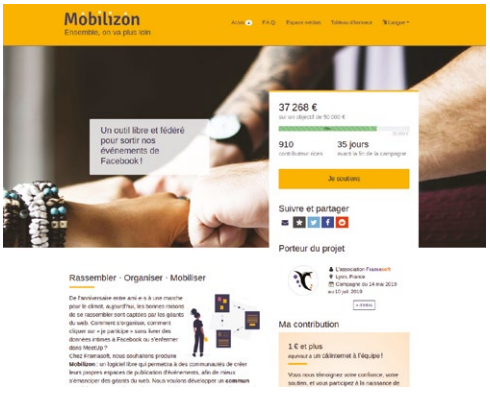
En bref...

LIBRE À VOUS ! : **L'ÉMISSION RADIO DE L'APRIL**

L'April, l'association de défense et de promotion du logiciel libre a sa propre émission radio pour discuter des sujets qui lui tiennent à cœur. Elle s'appelle « Libre à vous ! » et est diffusée tous les mardis de 15h30 à 17h sur la chaîne radio Cause commune (91.3 sur la bande FM en Île-de-France). Ce rendez-vous hebdomadaire est l'occasion d'échanger autour des dossiers juridiques et politiques menés par l'association ainsi que des actions réalisées par cette dernière.

Pour ne manquer aucun épisode, vous pouvez vous rendre sur **https://cause-commune.fm/shows/libre-a-vous/** où vous trouverez sous forme de podcasts les émissions précédemment diffusées. Une bande-annonce vous attend également à cette adresse pour découvrir l'émission. Bonne écoute ! ■

MOBILIZON, UN PROJET LIBRE ET FÉDÉRÉ POUR **ORGANISER SES ÉVÉNEMENTS**



L'association Framasoft poursuit son action militante en dévoilant un nouveau projet fédéré dont l'objectif est de fournir une plateforme de création d'événements que tout un chacun pourra s'approprier, loin des solutions proposées par les géants du Net et des scandales liés à l'utilisation de ces dernières.

Une campagne de crowdfunding (qui se poursuit jusqu'au 10 juillet) a été lancée pour pouvoir financer le lancement de ce projet qui se veut libre, éthique et développé dans le respect de la vie privée de ses utilisateurs. Cette plateforme qui offrira une solution pour rassembler, organiser et mobiliser devrait dans un premier temps voir le jour sous la forme d'une version bêta dès cet automne avant de proposer une première version au grand public durant le 1er semestre 2020. Rendez-vous sur **https://joinmobilizon.org/fr/** pour en savoir plus et peut-être apporter votre pierre à l'édifice ! ■

QWANT CAUSES : LORSQUE VOS RECHERCHES PERMETTENT DE **FINANCER DES ASSOCIATIONS**

Lancé en mai dernier, ce service permet de financer des projets en faisant des recherches via le moteur de recherche français Qwant. Les associations peuvent ainsi obtenir non seulement plus de visibilité, mais aussi une source de revenus supplémentaire pour mener à bien leurs actions.

Qwant Causes s'appuie sur la plateforme HelloAsso. Après inscription sur cette dernière, les associations doivent accepter d'apparaître sur les sites partenaires de la plateforme dont Qwant fait partie. Les internautes, de leur côté, activent le mode « donations » de leur moteur de recherche. Celui-ci va afficher des annonces publicitaires supplémentaires. Les revenus générés par celles-ci – appelés les « QOZ » – seront reversés aux associations sélectionnées par l'internaute ou, par défaut, à l'association du mois à la fin de chaque mois. Un compteur s'affiche dans le *header* du moteur de recherche permettant à l'internaute de suivre les donations réalisées par le biais de ses recherches. Direction **https://org.qwant.com/** en veillant à bien activer les « Qoz » pour découvrir cela ! ■

ACTUELLEMENT DISPONIBLE

LINUX PRATIQUE HORS-SÉRIE N°45

COMPRENDRE, UTILISER & ADMINISTRER LINUX
GNU LINUX PRATIQUE
HORS-SÉRIE N°45
JUIN JUILLET 2019
FRANCE MÉTRO. : 14,90 €
CH : 23.80 CHF
PORT : 15.90 €
MAR. : 165 MAD
DOM/S : 15,90 €
CAN : 23.99 $CAD
MODÉLISATION / UML
Générez votre code à partir de diagrammes de classes avec Modelio
CONTENEURS & VIRTUALISATION
POURQUOI ? QUAND ? COMMENT ?
▸DOCKER
Découvrez la technologie des conteneurs avec LXD et Docker
▸KUBERNETES
Orchestrez et automatisez le déploiement de vos conteneurs
▸VIRTUALBOX
Virtualisez n'importe quel système ou machine en toute simplicité
▸WINDOWS SUBSYSTEM LINUX
Intégrez un véritable système Linux au cœur de Windows
AUDIO / PRO
Utilisez le standard MIDI avec la station audio numérique Ardour
ACCESSIBILITÉ
Quels outils libres pour assister les personnes en situation de handicap ?
L 12225 - 45 H - F: 14,90 € - RD

NE LE MANQUEZ PAS

CHEZ VOTRE MARCHAND DE JOURNAUX ET SUR :

https://www.ed-diamond.com

Enregistrer le son
avec Audio Recorder

ANTHONY CARRÉ

Outil utilisé : Audio Recorder 3.0.5 - **Site du projet :** https://launchpad.net/~audio-recorder

POUR ENREGISTRER LE SON QUI SORT DE VOS ENCEINTES, CELUI D'UNE APPLICATION, D'UNE RADIO EN STREAMING OU DEPUIS UN MICROPHONE, IL EXISTE UN GRAND NOMBRE D'APPLICATIONS. SOUNDRECORDER DU BUREAU GNOME EST BEAUCOUP TROP BASIQUE, AUDACITY UNE USINE À GAZ POUR UNE SI SIMPLE ACTION, KWAVE À RÉSERVER AUX AFICIONADOS DE KDE. AUDIO RECORDER EST UNE APPLICATION SIMPLE À PRENDRE EN MAIN, MAIS PLEINE DE BONNES SURPRISES.

» ÉTAPE 1
INSTALLATION

Disponible directement sous forme de paquets dans certaines distributions (openSUSE par exemple), l'installation peut se faire d'autres façons pour les distributions ne le proposant pas depuis leur gestionnaire de paquets.

Les utilisateurs d'Ubuntu et dérivés pourront profiter du dépôt ppa:audio-recorder/ppa.

Les utilisateurs d'Archlinux et dérivés peuvent procéder à l'installation via leur assistant AUR préféré :

```
yay audio-recorder
```

Si votre distribution est compatible avec le système de paquets snap (snapd), vous pouvez installer

Audio Recorder (**https://snapcraft.io/audio-recorder**) assez simplement. Toutefois cette version rencontre quelques limitations : pas d'interface Mpris/Dbus, pas de format m4a… et surtout nous avons rencontré quelques bugs avec celle-ci lors de nos essais). Vous pouvez tout de même l'essayer via :

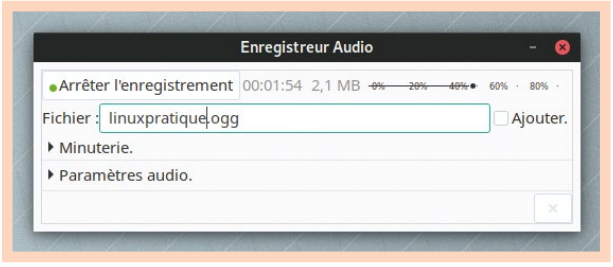
```
sudo snap install audio-recorder --beta
snap run audio-recorder
```

Enfin, vous pouvez compiler le logiciel depuis les sources, disponibles sous licence GPL3. Le code en cours de développement est téléchargeable via Bazaar :

```
bzr branch lp:audio-recorder
```

Suivez alors les instructions disponibles dans le fichier INSTALL.

» ÉTAPE 2 UTILISATION BASIQUE



Un bouton, une case à cocher et une case de saisie de texte (pour le nom de fichier), on peut dire que l'interface par défaut d'Audio Recorder est on ne peut plus simple !

Si vous ne saisissez pas de nom de fichier, celui-ci sera généré automatiquement (lors de nos essais, le nom de fichier saisi était d'ailleurs automatiquement remplacé par le format déterminé dans les préférences), par défaut l'enregistrement est stocké dans le dossier ~/Audio (qui peut être différent selon votre configuration ou ~/snap/audio-recorder/common/Audio pour une installation depuis snap).

La case à cocher ***Ajouter*** permet de cumuler vos enregistrements à la suite les uns des autres dans un seul et même fichier audio, si la case est décochée, un nouveau fichier sera créé chaque fois que vous cliquerez sur ***Commencer l'enregistrement***.

Lorsque l'enregistrement est lancé, la durée d'enregistrement, la taille du fichier et une barre horizontale graduée indiquant le niveau sonore apparaissent. Avec des clics sur cette barre représentant le son, gauche pour le format des graduations et droit pour le format de la barre, vous pouvez en changer l'apparence.

Deux menus complémentaires peuvent être dépliés pour apporter des fonctions supplémentaires : ***Minuterie*** et ***Paramètres audio.***

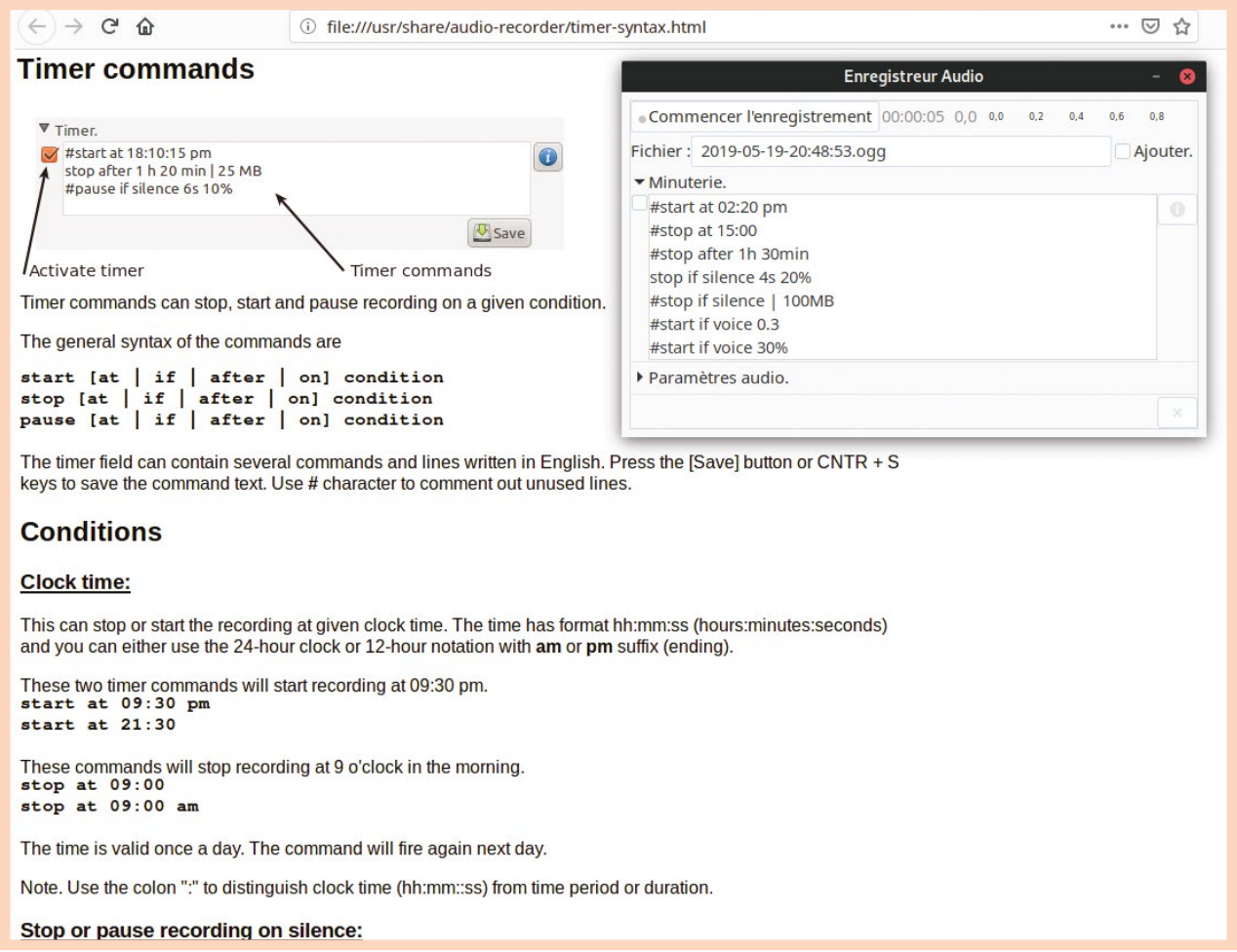
» ÉTAPE 3 MINUTERIE

Minuterie est une option bien plus puissante que ce que son nom ne pourrait le laisser croire, elle ajoute trois items à l'interface :

- une case à cocher qui permet d'activer/désactiver la fonction ;
- un bouton d'aide pour afficher quelques compléments d'informations ;
- une boîte de saisie de texte permettant de définir la commande de minuterie. Elle contient déjà plusieurs lignes d'exemples et une ligne active : les lignes commençant par un # sont des lignes commentées, elles ne sont pas prises en compte, mais vous permettent d'expliciter la syntaxe par l'exemple.

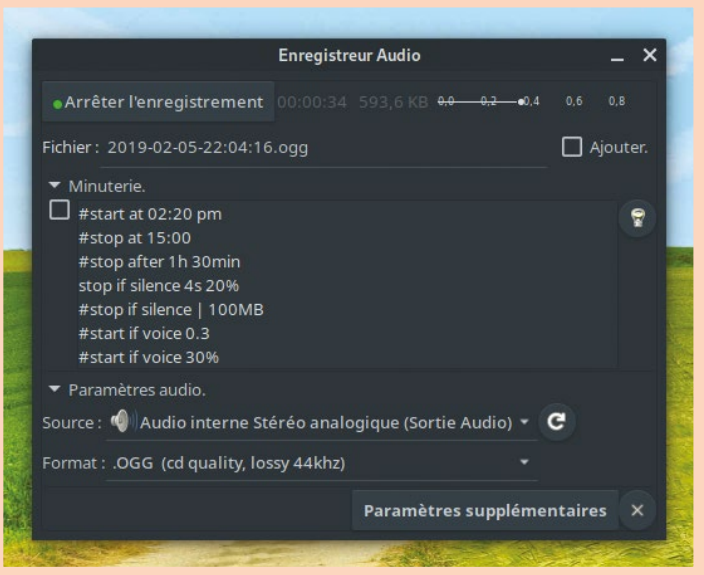
Les possibilités sont très nombreuses, car la variété des commandes ainsi saisies est bien plus vaste qu'un simple choix de délai ou d'horaires. Vous pouvez d'ailleurs activer plusieurs commandes en même temps pour automatiser au maximum vos enregistrements. Voici deux exemples de règles assez représentatives des possibilités…

En saisissant start if sound 0.3 dans le champ ***Minuteur***, l'enregistrement démarrera automatiquement lorsque le son détecté dépassera 30 % du volume maximum. Avec stop if silence 3s -32dB, l'enregistrement s'arrêtera automatiquement si un silence est détecté


file:///usr/share/audio-recorder/timer-syntax.html
Timer commands
Timer.
#start at 18:10:15 pm
stop after 1 h 20 min | 25 MB
#pause if silence 6s 10%
Save
Activate timer
Timer commands
Timer commands can stop, start and pause recording on a given condition.
The general syntax of the commands are
start [at | if | after | on] condition
stop [at | if | after | on] condition
pause [at | if | after | on] condition
The timer field can contain several commands and lines written in English. Press the [Save] button or CNTR + S keys to save the command text. Use # character to comment out unused lines.
Conditions
Clock time:
This can stop or start the recording at given clock time. The time has format hh:mm:ss (hours:minutes:seconds) and you can either use the 24-hour clock or 12-hour notation with am or pm suffix (ending).
These two timer commands will start recording at 09:30 pm.
start at 09:30 pm
start at 21:30
These commands will stop recording at 9 o'clock in the morning.
stop at 09:00
stop at 09:00 am
The time is valid once a day. The command will fire again next day.
Note. Use the colon ":" to distinguish clock time (hh:mm::ss) from time period or duration.
Stop or pause recording on silence:
Enregistreur Audio
Commencer l'enregistrement 00:00:05 0,0
Fichier : 2019-05-19-20:48:53.ogg
Ajouter.
Minuterie.
#start at 02:20 pm
#stop at 15:00
#stop after 1h 30min
stop if silence 4s 20%
#stop if silence | 100MB
#start if voice 0.3
#start if voice 30%
Paramètres audio.

trois secondes (en spécifiant le seuil à partir duquel on considère un silence).

Vous pouvez ainsi définir une taille de fichier maximum, mettre en pause lors des silences, arrêter après un certain temps, reprendre à une certaine heure…



» ÉTAPE 4
PARAMÈTRES AUDIO

Le menu déroulant ***Paramètres audio*** permet de personnaliser les deux paramètres les plus importants pour un enregistrement audio :

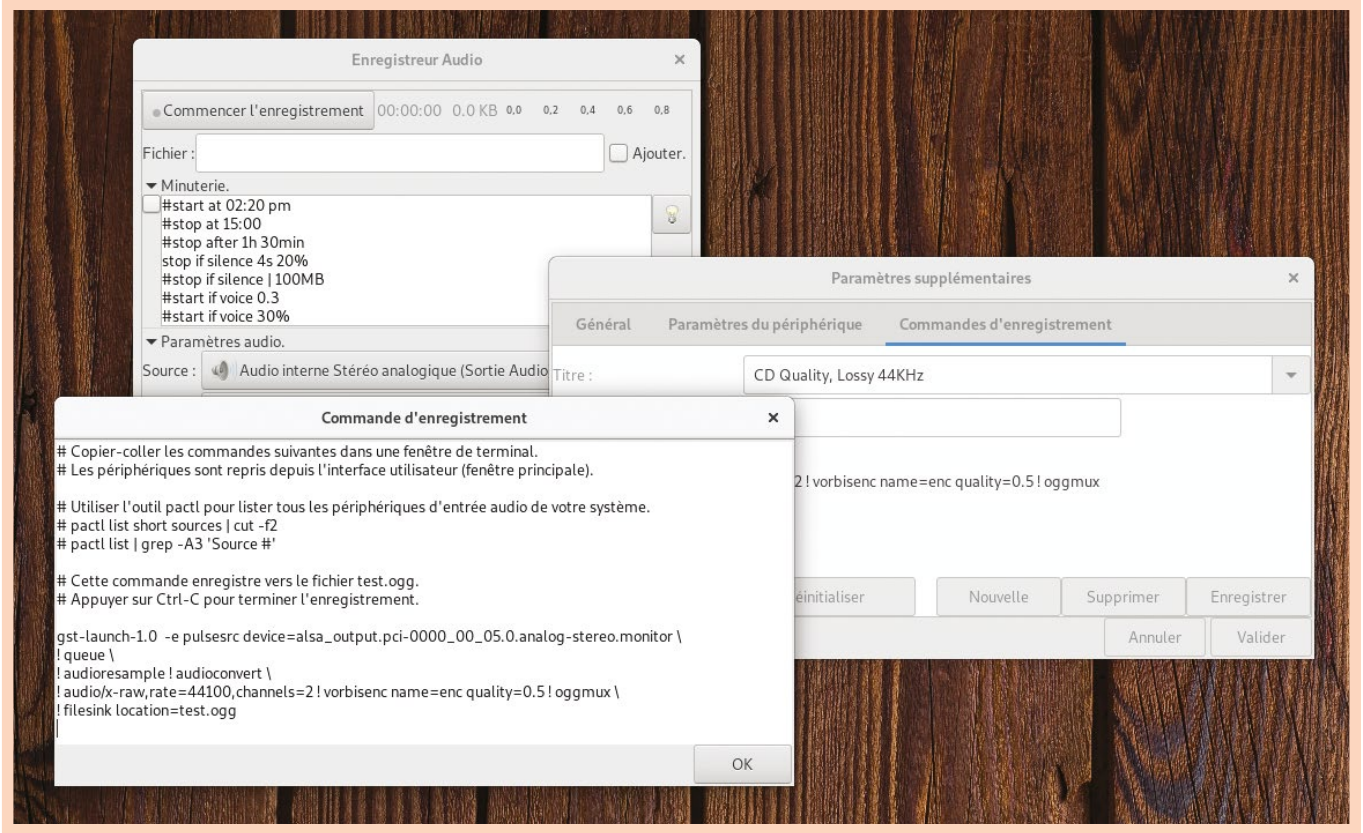
- la source audio d'entrée qui sera utilisée pour l'enregistrement : webcam, microphone, sortie audio, etc. Un bouton permet de rafraîchir la liste des entrées disponibles ;
- le format d'encodage : ogg, m4a, flac, mp3, wav ou spx, nous supposons qu'au moins l'un de ces formats vous conviendra.

En déroulant le menu ***Paramètres audio***, vous accédez également à un bouton additionnel : ***Paramètres supplémentaires***.

» ÉTAPE 5 PARAMÈTRES SUPPLÉMENTAIRES

Ce menu équivaut plus ou moins au menu « Préférences » de bon nombre d'applications et autorise assez logiquement la personnalisation de nombreux paramètres avancés, que nous ne détaillerons pas ici.

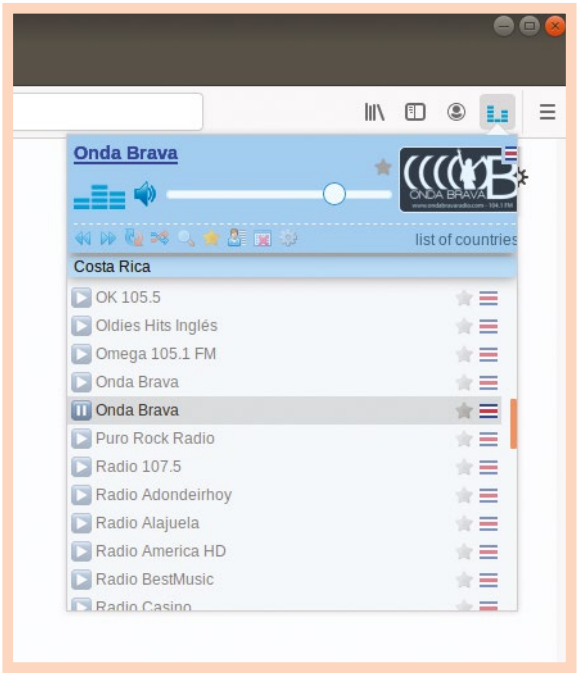
Là, où le logiciel se démarque, c'est dans l'onglet ***Commandes d'enregistrement***, puisqu'on y trouve un bouton assez original. Audio-recorder n'est ni plus ni moins qu'une interface graphique simplifiant l'usage de quelques commandes CLI. Si vous souhaitez scripter vos enregistrements vous pourriez apprécier d'avoir accès aux commandes lancées par le logiciel pour en copier/coller la structure. C'est exactement ce que propose le bouton ***Afficher commande***. Trop peu de GUI proposent cette très appréciable fonctionnalité ! ■

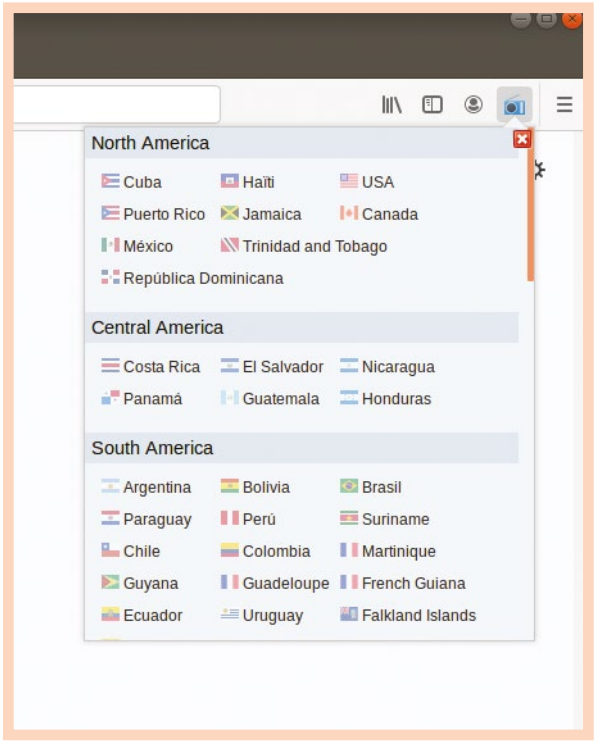

Enregistreur Audio
Commencer l'enregistrement
00:00:00 0.0 KB
Fichier :
Ajouter.
Minuterie.
#start at 02:20 pm
#stop at 15:00
#stop after 1h 30min
stop if silence 4s 20%
#stop if silence | 100MB
#start if voice 0.3
#start if voice 30%
Paramètres audio.
Source :
Audio interne Stéréo analogique (Sortie Audio
Paramètres supplémentaires
Général
Paramètres du périphérique
Commandes d'enregistrement
Titre :
CD Quality, Lossy 44KHz
2 ! vorbisenc name=enc quality=0.5 ! oggmux
Nouvelle
Supprimer
Enregistrer
Annuler
Valider
Commande d'enregistrement
Copier-coller les commandes suivantes dans une fenêtre de terminal.
Les périphériques sont repris depuis l'interface utilisateur (fenêtre principale).
Utiliser l'outil pactl pour lister tous les périphériques d'entrée audio de votre système.
pactl list short sources | cut -f2
pactl list | grep -A3 'Source #'
Cette commande enregistre vers le fichier test.ogg.
Appuyer sur Ctrl-C pour terminer l'enregistrement.
gst-launch-1.0 -e pulsesrc device=alsa_output.pci-0000_00_05.0.analog-stereo.monitor \
! queue \
! audioresample ! audioconvert \
! audio/x-raw,rate=44100,channels=2 ! vorbisenc name=enc quality=0.5 ! oggmux \
! filesink location=test.ogg
OK

Worldwide Radio

LES RADIOS DU MONDE ENTIER EN UN TOUR DE MAIN

Disponible pour Firefox et Chrome/Chromium, Worldwide Radio vous permettra de profiter d'un large choix de stations radio à travers le monde en quelques clics. Le module se présente sous la forme d'une petite radio dans la barre d'état de votre navigateur web. Un clic sur celle-ci affiche les continents puis les pays pour lesquels des chaînes radio sont disponibles.





Il s'agit ensuite simplement de sélectionner un pays pour voir s'afficher la liste des radios proposées accompagnée d'un player. Une pop-up s'affiche au survol de chaque radio permettant ainsi d'obtenir un descriptif rapide de la chaîne en question. À gauche, on lance l'écoute de la station, à droite l'icône sous forme d'étoile permet de conserver celle-ci en tant que favori.

Le player s'accompagne de quelques options pratiques : le passage à la radio précédente ou suivante de la liste, la lecture aléatoire d'une station, l'accès rapide à ses favoris, le mode shuffle… Un outil de recherche est aussi de la partie pour trouver rapidement la radio de son choix.

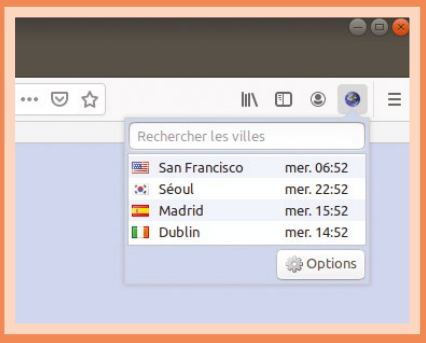
L'extension Worldwide Radio vous permet ainsi de découvrir de nouvelles stations étrangères ou retrouver tout simplement les chaînes que vous appréciez écouter en deux clics depuis votre navigateur. ■

VERSION TESTÉE : 2.6 **SITE DU PROJET :** http://forums.mozillazine.org/viewtopic.php?t=3039738

COMPATIBILITÉ : Firefox, Chrome/Chromium

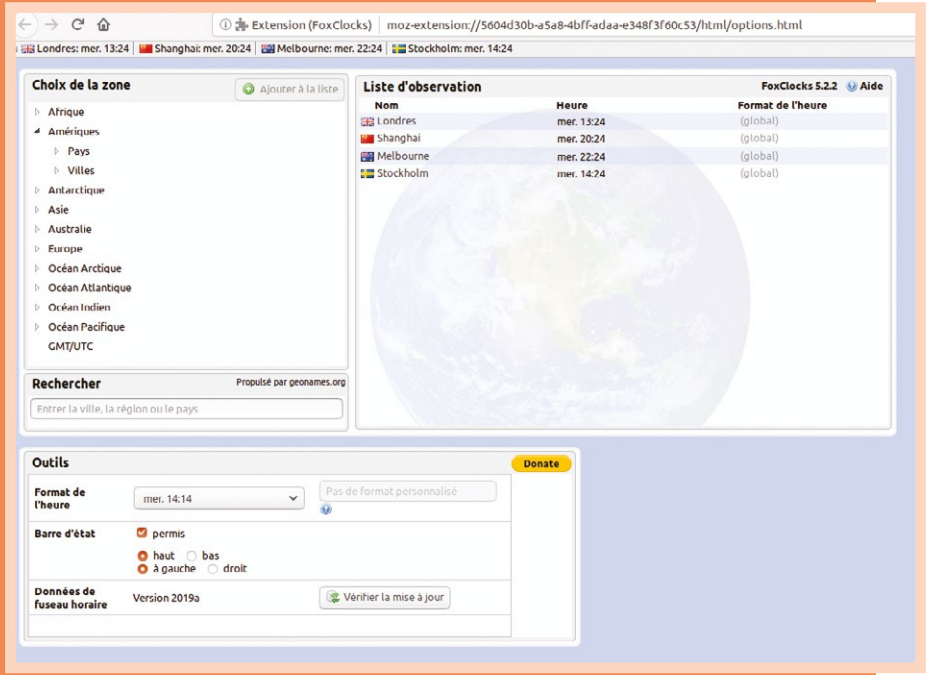
FoxClocks

POUR ÊTRE À L'HEURE AUX QUATRE COINS DE LA PLANÈTE



Utile si vous travaillez avec des collaborateurs aux quatre coins de la planète ou si vous avez de la famille ou des amis disséminés sur divers pays/continents, FoxClocks se présente sous la forme d'une extension pour les navigateurs Firefox et Chrome/Chromium dont le but est de vous fournir une horloge mondiale que vous pourrez personnaliser au gré de vos envies.

Une fois installée, elle prend la forme d'un petit globe dans la barre d'état de votre navigateur. Un clic sur celui-ci vous permettra d'accéder aux paramètres du module. Vous pourrez par ce biais choisir d'afficher les heures des pays/villes de votre choix en parcourant la liste fournie ou en tapant directement dans le moteur de recherche présent la localisation géographique souhaitée. L'idée est de pouvoir ainsi vous concocter votre propre « liste d'observation » composée des emplacements dont les fuseaux horaires vous intéressent. Un jeu d'options supplémentaire vous permettra ensuite de définir le format de l'heure que vous préférez afficher parmi une liste ou de personnaliser ce dernier. Enfin, vous pourrez également déterminer l'emplacement de ces indications horaires dans votre navigateur. Vous n'avez désormais plus aucune raison de ne pas être à l'heure pour vos visioconférences avec vos contacts éloignés ! ■



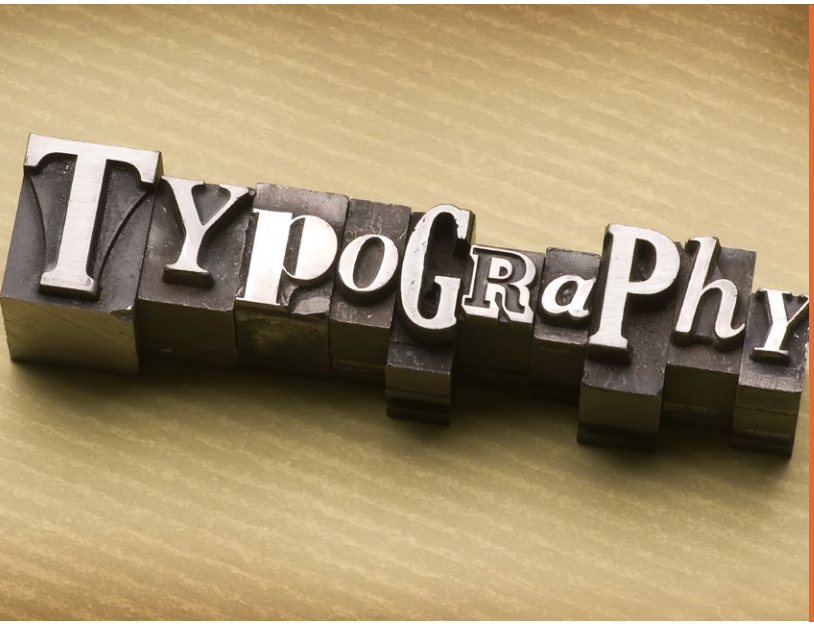
VERSION TESTÉE : 5.2.2 **SITE DU PROJET :** https://foxclocks.org/

COMPATIBILITÉ : Firefox, Chrome/Chromium

Modifiez et créez vos propres polices avec FontForge

YANN MORÈRE

Outil utilisé : FontForge July 2018 - **Site du projet :** https://fontforge.github.io/en-US/



IL EXISTE DES MILLIERS DE POLICES DE CARACTÈRES LIBRES D'ACCÈS SUR INTERNET. CEPENDANT, CERTAINES NE SONT PAS LIBRES DE DROITS OU ENCORE NE POSSÈDENT PAS LES CARACTÈRES ACCENTUÉS ET DEVIENNENT DE FAIT INUTILISABLES EN LANGUE FRANÇAISE. CRÉER UNE FONTE PERSONNALISÉE PEUT ÊTRE UN PLUS POUR VOUS DÉMARQUER GRAPHIQUEMENT. VOYONS COMMENT FONTFORGE VA NOUS PERMETTRE DE RÉALISER TOUT CELA.

» ÉTAPE 0 COMPRENDRE LA TYPOGRAPHIE ET SA TERMINOLOGIE

La conception de caractères est très complexe et très technique. Cependant à l'aide d'un outil pratique comme FontForge il est très facile pour un débutant de créer sa propre fonte. Mais il pourra aussi servir à des professionnels de l'édition, car il dispose d'un ensemble d'outils spécifiques et avancés.

Avant d'aller plus loin, il est nécessaire de préciser quelques termes importants. En effet, le domaine de la typographie est vaste et son vocabulaire riche peut vite devenir un jargon obscur.

La typographie est la composante artistique de l'écriture, c'est-à-dire l'expression de la lettre, la façon de représenter l'alphabet. Une typographie représente le plus souvent la création d'un style d'alphabet, et non d'un nouveau principe d'alphabet.

La fonte est appelée ainsi, car elle est historiquement issue de la fonte de plomb et d'antimoine pour générer les lettres pour l'imprimerie. Le mot désigne aujourd'hui le fichier numérique grâce auquel on peut utiliser la typographie. À noter qu'à une typographie peut correspondre plusieurs fontes. On parle aussi de famille de fontes. Elles sont autant de variantes. Les plus courantes sont le romain, le gras, l'italique et le gras italique.

Le caractère désigne un signe tracé ou écrit, qu'il soit une lettre, un signe de ponctuation, un chiffre, un symbole, etc. Il s'agit de la zone standardisée où l'un des éléments constitutifs du système d'écriture est défini (il y a bien sûr souvent plusieurs caractères par fonte, afin que celle-ci soit utilisable pour former des mots à l'écran) **[5]**.

Le glyphe est la forme graphique composée de contours que peut revêtir un caractère (il peut y avoir plusieurs glyphes par caractère, plusieurs a minuscules par exemple, ou plusieurs styles de chiffres).

Les capitales sont également appelées lettres majuscules. Les bas de casse ou lettres minuscules, sont ainsi appelées pour des raisons historiques. En effet, la casse était le meuble qui servait à stocker les caractères en plomb, avec en haut les capitales et en bas les minuscules, ou bas-de-casse.

Les petites capitales sont des versions miniatures des capitales et non pas des capitales réduites. Leur taille les rend plus discrètes que les capitales normales.

Figure 1

Les ligatures sont des combinaisons de deux ou trois lettres consécutives pour ne former qu'un caractère. Les combinaisons classiques sont le « ff », « fi », « ffi » et « ffl » (Figure 1).

La création de fontes est une démarche particulière, car elle est prévue pour être partagée, utilisée par d'autres personnes dans divers contextes. Le choix du nom de fonte revêt une importance particulière. Le fait de choisir un nom original permet à l'auteur de démarquer sa création du reste des autres fontes. Le nom peut être la combinaison d'éléments culturels (origine géographique, période, hommage ou parodie d'autres fontes) afin de lui donner un caractère unique.

On distinguera le nom interne de la fonte (celui qui apparaît dans le menu d'un traitement de texte ou d'un logiciel de dessin vectoriel) et le nom des fichiers de la fonte.

» ÉTAPE 1
INSTALLER ET GÉRER VOS FONTES

Il est possible d'installer les fontes courantes directement à partir du gestionnaire de paquets de votre distribution Linux. La plupart du temps, les noms des paquets se terminent par -font :

```
$ pacman -Ss font
extra/adobe-source-code-pro-fonts 2.030ro+1.050it-4
    Monospaced font family for user interface and coding
environments
extra/adobe-source-sans-pro-fonts 2.040ro+1.090it-1
    Sans serif font family for user interface environments
extra/adobe-source-serif-pro-fonts 2.007ro+1.007it-2
    Serif typeface for setting text. Designed to complement
Source Sans Pro
extra/artwiz-fonts 1.3-10 [installed]
    This is set of (improved) artwiz fonts
extra/bdf-unifont 11.0.03-1
[...]
```

Les fontes installées dans votre système d'exploitation sont stockées dans le répertoire /usr/share/fonts/ et sont classées par type :

```
$ ls /usr/share/fonts/
100dpi  75dpi  artwiz-fonts  cantarell  cyrillic  encodings
gsfonts  misc  oiio  OpenImageIO  OTF  speedo  TTF  Type1  util
```

Il existe des fontes bitmaps pour l'affichage graphique sur écran (100dpi, 75dpi), les fontes de type connu comme TTF (*True Type Font*) ou OTF (*Open Type Font*), les fontes PostScript Type 1 destinées aux imprimantes…

Si vous désirez ajouter une fonte qui ne n'est pas disponible par l'intermédiaire d'un paquet, il vous est possible de la télécharger sur l'un des nombreux sites dédiés : Open Font Library, DaFont, Google Fonts, Abstrac Fonts, etc.

Les formats les plus courants qu'il est possible d'installer sont les suivants : ttf, otf et pfb (type1). Une fois téléchargés et désarchivés, on place les fichiers souhaités dans le répertoire .local/share/fonts du dossier personnel. Pour être certain qu'elles soient bien prises en compte, on utilise la commande suivante :

```
$ fc-cache -f -v
```

Les fontes seront alors disponibles pour l'utilisateur courant.

» REMARQUE
Il est possible de placer les fontes dans le répertoire ~/.fonts. Les manipulations restent identiques.

Si vous désirez rendre disponibles les fontes pour l'ensemble des utilisateurs du système, vous devez installer les fichiers correspondants dans l'un des sous-répertoires de /usr/share/fonts correspondant au format de la fonte. Relancez ensuite la commande fc-cache pour une prise en compte immédiate.

Il est aussi possible d'installer des fontes de manière graphique à l'aide de l'application fontmanager qui se trouve dans les dépôts de votre distribution. Je vous laisse découvrir cette application par vous-même.

» ÉTAPE 2
INSTALLER FONTFORGE ET ÉDITER UNE FONTE

Afin de pouvoir travailler convenablement, nous allons installer les outils nécessaires à l'utilisation de FontForge **[2]**. Sur une distribution de type Ubuntu, il suffira d'installer le paquet suivant :

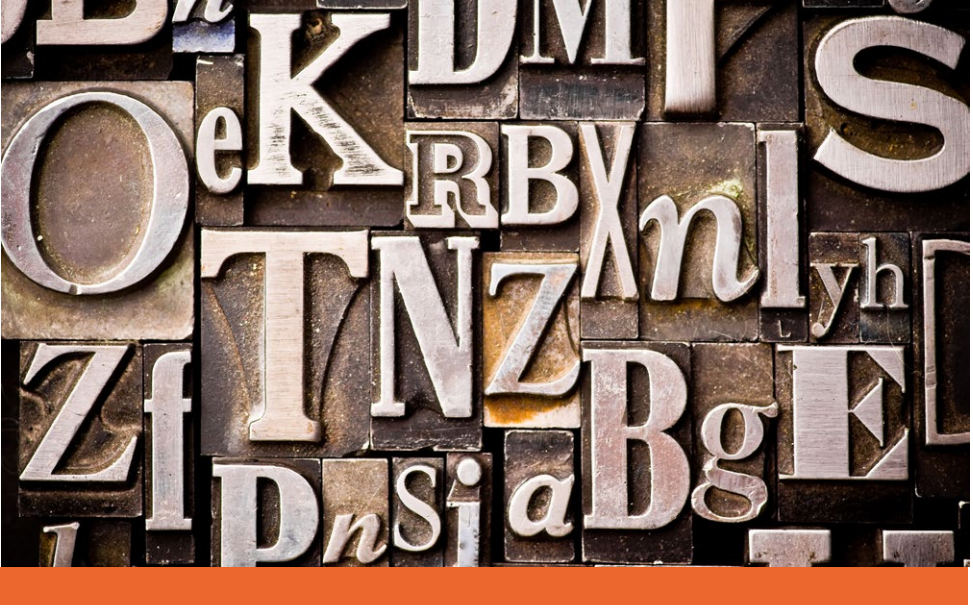
```
$ sudo apt-get install fontforge
```

Sur ma distribution Arch Linux, la commande est la suivante :

```
$ sudo pacman -S fontforge
```

» REMARQUE
Pour la rédaction de cet article, j'ai utilisé la version de juillet 2018 disponible sur ma distribution Arch Linux.

Figure 2



On lance FontForge à l'aide de la commande éponyme :

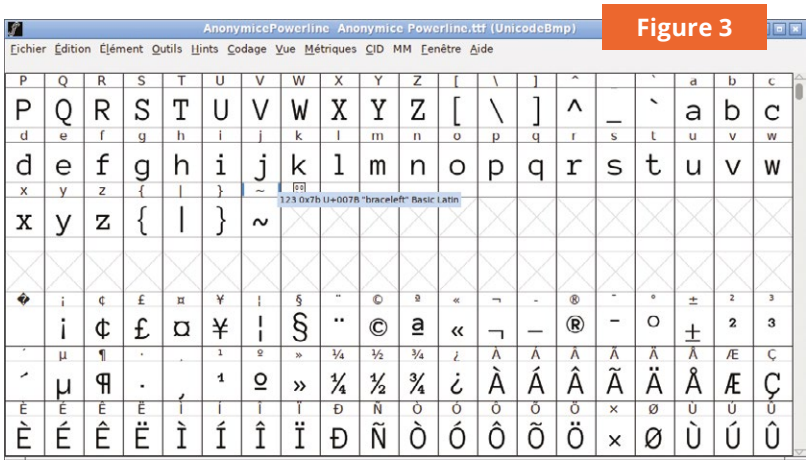
```
$ fontforge
```

On obtient le résultat de la figure 2.

La fenêtre FontForge se ferme automatiquement au bout de quelques secondes. Le logiciel nous demande alors d'ouvrir la fonte à éditer ou alors de créer une nouvelle fonte par l'intermédiaire de la fenêtre ***Ouvrir fonte***. Comme toutes les fontes installées localement pour votre utilisateur se trouvent dans un répertoire caché, nous allons les afficher dans l'interface en cochant ***Montrer les fichiers cachés***, en cliquant sur le bouton « roue dentée » en haut à droite de l'interface. Ensuite, on sélectionne une police TTF présente sur le système dans le répertoire .local/share/fonts. On obtient le résultat de la figure 3.

Cette fenêtre de fonte est la fenêtre principale. Elle se présente sous la forme d'une table de glyphes, organisés selon le codage de leur emplacement. Le codage définit le nombre d'emplacements et la place des glyphes dans ces emplacements. Ils peuvent varier sensiblement d'un codage à l'autre. Il est donc conseillé d'utiliser le codage Unicode. Les informations permettant d'identifier les cases de glyphes sont affichées. Elles sont composées de la valeur d'index, son équivalent hexadécimal, le code du caractère Unicode correspondant, le nom de glyphe et le nom du caractère Unicode correspondant.

Figure 3


AnonymicePowerline Anonymice Powerline.ttf (UnicodeBmp)
Fichier Edition Élément Outils Hints Codage Vue Métriques CID MM Fenêtre Aide

» REMARQUE
Il est possible de sélectionner plusieurs fontes simultanément en maintenant la touche [Maj].

Le fait de double-cliquer sur l'une des cases ouvre la fenêtre d'édition du glyphe de la lettre. Celle-ci permet de modifier le contour d'un glyphe. Vous pouvez en ouvrir plusieurs, mais une même fenêtre de glyphe peut aussi avoir plusieurs onglets spécifiques à plusieurs glyphes. Cela permet de travailler avec plusieurs fenêtres, ou une seule. La figure 4, page suivante présente un exemple de fenêtre d'édition de glyphe.

Les composants supplémentaires de la fenêtre de glyphes sont les informations du curseur (position, déplacement, etc.), les règles horizontales (avec position du curseur), la fenêtre graphique (canevas) contenant le contour, les dessins de contours composés des points et lignes, la ligne de base et les approches gauche (depuis x=0) et droite (jusqu'à la chasse, largeur du glyphe courant ou distance entre le début d'un glyphe et le début du glyphe suivant).

Le canevas de dessin est la zone qui affiche le calque sélectionné (***Guide***, ***Arrière***, ***Avant***) et les contours qu'il contient. Ces derniers sont modifiables par l'intermédiaire de la palette d'outils à gauche de l'interface. Les autres calques peuvent être visibles, mais leurs contours ne le sont pas.

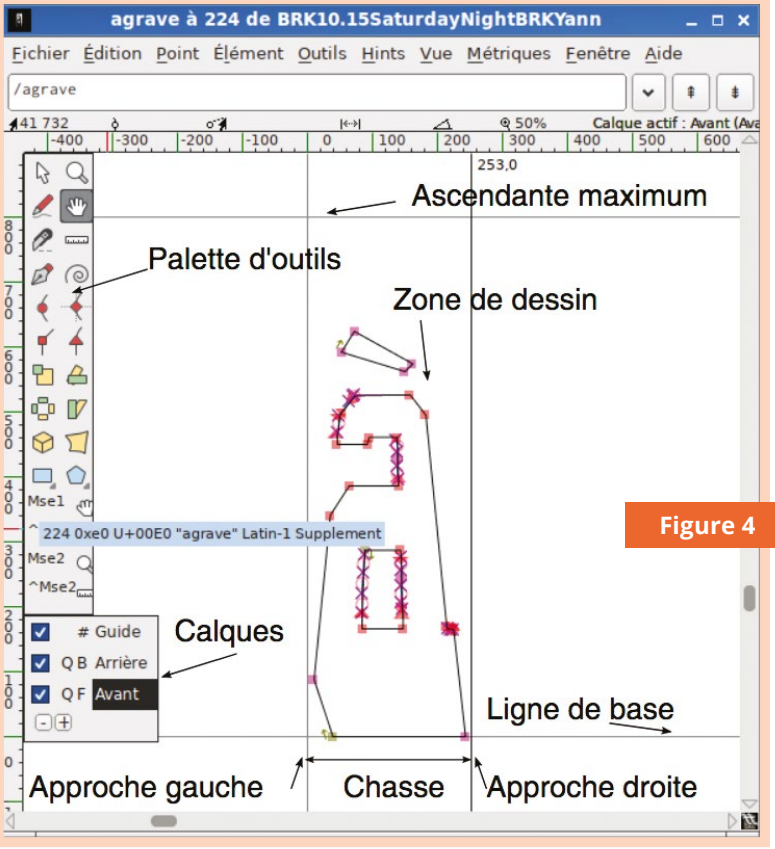


Figure 4

La fenêtre de glyphe contient un menu quasiment identique à celui décrit dans la fenêtre principale. Un nouveau menu ***Point*** permet de convertir le type de point des points sélectionnés, de changer le premier point d'un contour, de convertir en ligne et de convertir en arc entre autres. Le menu ***Élément*** est lui aussi plus complet et donne accès à des opérations spécifiques aux glyphes et à leur modification.

Pour un descriptif plus complet des outils contenus dans ces menus, je vous renvoie vers la documentation officielle à l'adresse **[3]**.

Voyons maintenant comment modifier une fonte existante qui ne possède pas les accentuations.

» ÉTAPE 3
MODIFIER UNE FONTE EXISTANTE

Lorsque vous téléchargez des fontes gratuites, elles ont très souvent été réalisées par des anglophones qui ne se soucient pas des caractères accentués.

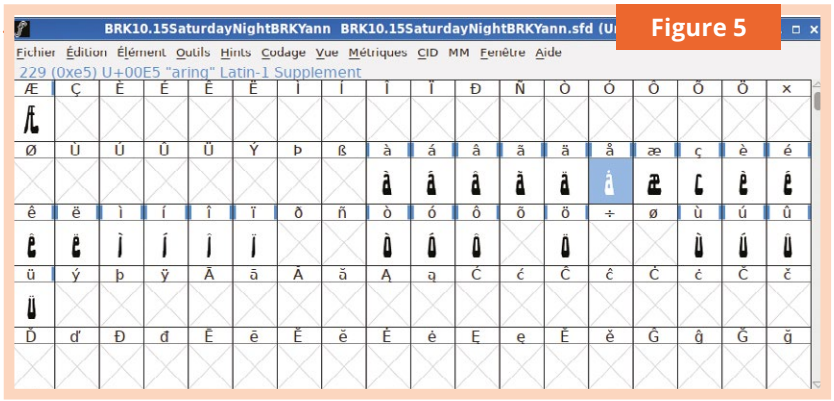

BRK10.15SaturdayNightBRKYann BRK10.15SaturdayNightBRKYann.sfd
Fichier Édition Élément Outils Hints Codage Vue Métriques CID MM Fenêtre Aide
229 (0xe5) U+00E5 "aring" Latin-1 Supplement

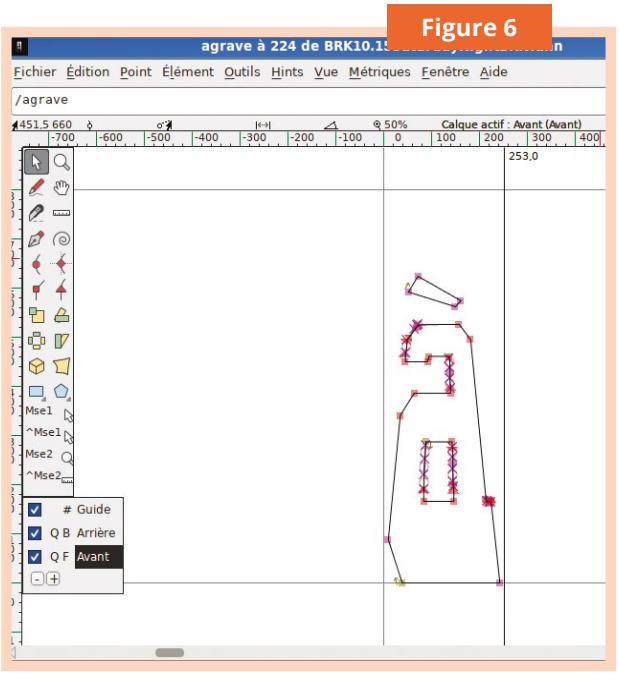
Figure 5

Lorsque vous utilisez ces fontes, comme les caractères accentués ne sont pas présents, le résultat est souvent surprenant et la fonte est inutilisable la plupart du temps dans les langues latines. Nous allons donc ajouter les caractères manquants.

Pour cela, on commence par ouvrir la fonte initiale à l'aide de FontForge. On remarque qu'effectivement les caractères accentués français ne sont pas définis. Nous allons les ajouter pour obtenir le résultat de la figure 5.

Afin de minimiser le travail à réaliser, on va juste ajouter les accents des voyelles en les copiant dans les cases idoines. Un simple copier-coller de case de la lettre sans accent vers la lettre accentuée permet de réaliser l'opération. Ensuite, on double clique sur la case de la lettre accentuée à modifier afin d'ouvrir la fenêtre d'édition de glyphes. À l'aide de vos talents d'artiste graphique, vous allez dessiner un accent à cette lettre dans l'esprit de la fonte. Pour cela, on va utiliser les outils de dessin mis à notre disposition dans l'interface. Un exemple est donné en figure 6.

Figure 6


Fichier Édition Point Élément Outils Hints Vue Métriques Fenêtre Aide
/agrave
Calque actif : Avant (Avant)
Guide
Q B Arrière
Q F Avant

Il faut maintenant réitérer cette opération pour toutes les lettres accentuées dont vous aurez besoin. On se facilitera la tâche en utilisant les outils de symétrie. Par exemple, pour passer de l'accent grave à l'accent aigu on réalise une copie de la lettre à l'accent grave, on sélectionne la partie du glyphe correspondant à l'accent et on opère une symétrie horizontale à l'aide de l'outil de symétrie.

On réitère ensuite pour « â », « ä », « ã », « å » et les autres voyelles. C'est un travail un peu long, mais il n'y a pas d'autre solution. À chaque étape, vous pouvez enregistrer vos modifications dans un format de fichier spécifique à FontForge (.sfd).

L'étape suivante consiste à exporter la fonte dans un format utilisable par vos logiciels de traitement de texte ou de composition graphique (Inkscape, GIMP, etc.). Afin de ne pas générer de conflit entre la fonte initiale et celle modifiée que vous allez générer, il est nécessaire de modifier le nom de fonte qui sera embarqué à l'intérieur du fichier de fonte. C'est ce nom qui est utilisé par les logiciels lorsqu'ils vous présentent la liste des fontes utilisables. En effet, si vous modifiez simplement le nom de fichier de la fonte généré (mafontmodifiee.ttf par exemple), à l'intérieur des logiciels, vous aurez du mal à faire la différence entre la fonte initiale et la fonte modifiée, car elles possèderont le même nom. Pour cela, il faut se rendre dans le menu ***Outils > Infos*** fonte qui nous affiche la Figure 7.

Il suffit de modifier le nom de la famille de la fonte ainsi que le nom de la fonte. Ensuite, on génère la fonte à l'aide du menu ***Fichier > Générer fonte*** ou le raccourci [Shift]+[Ctrl]+[G]. Il faut alors choisir le type de fichier de fonte désiré. J'ai opté pour le format d'origine *True Type Font* (TTF). Mais vous avez accès à un grand nombre de formats d'enregistrement différents (PostScript, Mac, SVG, etc.).

Si vous cochez la case ***Validation avant d'enregistrer***, FontForge réalisera un ensemble de vérification avant de générer la fonte. Dans notre cas, cela générera des messages d'avertissement, car nous n'avons pas ajouté l'ensemble des caractères accentués. Finalement, on clique sur le bouton ***Générer*** pour

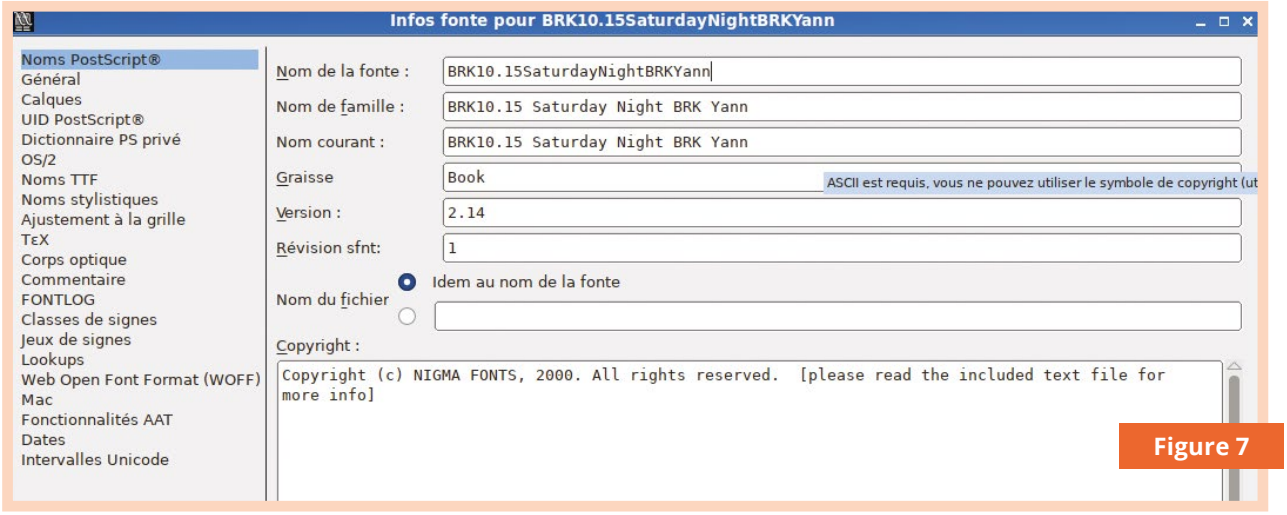


Figure 7

produire le fichier BRK10.15SaturdayNightBRKYann.ttf. On le copie ensuite dans le répertoire ~/.local/share/fonts et on relance fc-cache pour mettre à jour la liste des fontes disponibles :

```
$ cp BRK10.15SaturdayNightBRKYann.ttf
~/.local/share/fonts
$ fc-cache -f -v
```

Nous allons maintenant tester notre fonte modifiée dans le logiciel de dessin vectoriel Inkscape afin de vérifier que les caractères accentués sont bien présents et utilisables. En cas de problème, il faut rééditer la fonte, la modifier et la générer à nouveau.

Maintenant que nous avons pris en main FontForge pour la modification d'une fonte, voyons comment créer notre propre fonte.

» ÉTAPE 4
CRÉER SA PROPRE FONTE

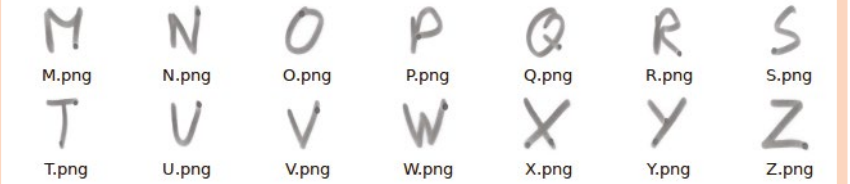
Dans cette partie, la méthode présentée n'est peut-être pas la meilleure ni la plus rapide, mais elle permet simplement et avec des outils libres de créer sa propre fonte à l'aide de votre propre écriture manuscrite.

Pour cela, il faut dans un premier temps écrire l'ensemble des lettres qui composeront votre fonte. On peut s'aider des tables de liste de caractères Unicode à l'adresse **[4]** afin de ne pas oublier de caractères. Pour la langue française, on pourra se contenter des tables « Contrôles C0 et latin de base » et « Contrôles C1 et supplément latin-1 ».

Ensuite, pour avoir des lettres de taille similaire, il est préférable de les dessiner sur un calque en ayant préalablement placé dessous une grille. Si vous avez une table lumineuse sous la main c'est encore mieux. J'ai utilisé un marqueur noir pour écrire les lettres sur le calque. Cela permet d'avoir une bonne épaisseur de trait. Pour l'exemple, je n'ai écrit, ni les lettres accentuées, ni la ponctuation. Bien sûr, pour que votre police soit complète, il est impératif d'être exhaustif.

Ensuite, on scanne le calque et on sépare chaque lettre dans un fichier PNG spécifique (Figure 8). L'étape suivante consiste à « vectoriser » chaque glyphe. Pour cela, on utilise Inkscape qui possède un très bon outil de « vectorisation » intégré. On affiche la fenêtre idoine à l'aide du menu ***Chemin > Vectoriser un objet matriciel*** ou par le raccourci [Alt]+[Maj]+[B] (Figure 9).

Figure 8



À partir de cet instant, les choses vont devenir répétitives pour chacun des glyphes à intégrer dans la fonte :

- on importe le fichier bitmap du glyphe dans Inkscape : ***Fichier > Importer*** ou [Ctrl]+[I] ;
- on « vectorise » à l'aide des paramètres indiqués dans la figure 14 ;
- on copie/colle le glyphe vectorisé dans un nouveau fichier Inkscape ([Ctrl]+[C], [Ctrl]+[N], [Ctrl]+[V]) ;
- on ajuste ensuite la page au contenu par le menu ***Fichier > Propriétés du Document***, item ***Redimensionner la page au contenu*** et on clique sur le bouton ***Ajuster la page au dessin ou à la sélection*** ;
- on enregistre le glyphe dans un fichier SVG du même nom.

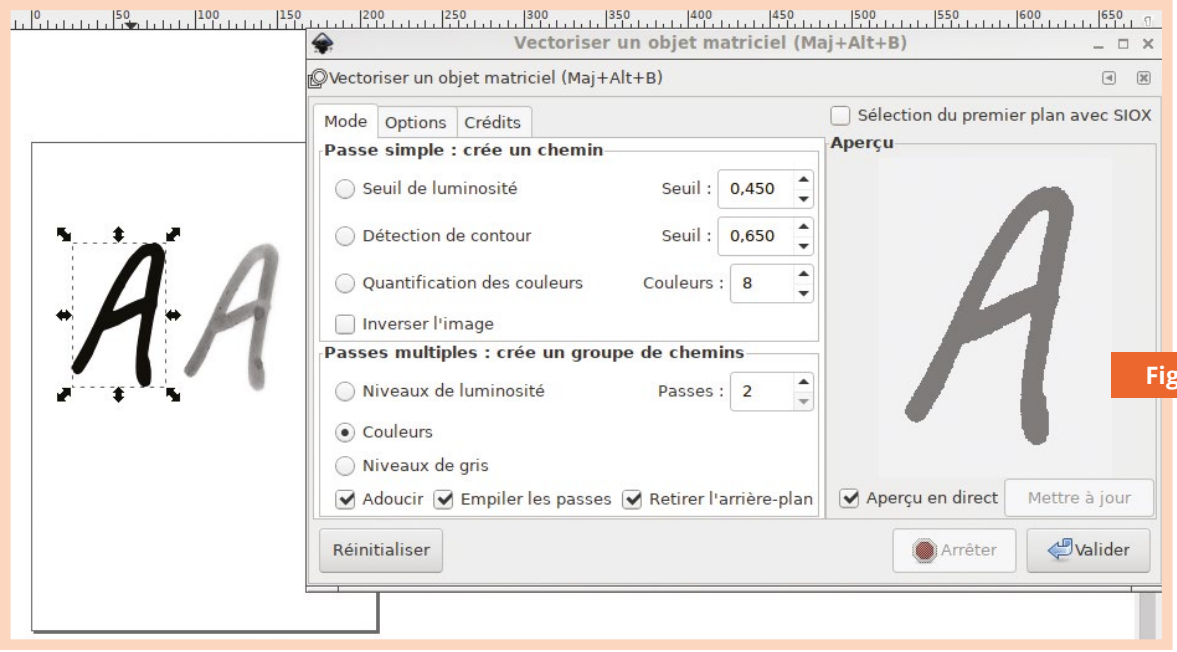


Figure 9

On dispose maintenant d'un ensemble de fichier SVG contenant tous les glyphes de notre fonte. Nous allons les importer dans une fonte nouvellement créée à l'aide de FontForge.

Une fois le logiciel exécuté, on clique sur le bouton ***Nouvelle fonte*** et une table de glyphes vierge de toutes lettres apparaît. Afin d'importer le glyphe correspondant à la lettre, on double-clique sur la case de la lettre à insérer. La fenêtre d'édition de glyphe s'ouvre et elle est vide. À l'aide du menu ***Fichier > Importer***, on sélectionne le fichier SVG correspondant à notre lettre et l'on clique sur importer. Le tracé du glyphe importé apparaît (Figure 10). On peut alors ajuster l'approche droite et gauche à sa convenance afin que l'espace entre les lettres étroites ne soit pas trop grand (« I », « S », « U » etc.). Après avoir fermé la fenêtre de glyphe, on vérifie que la case de la lettre est bien remplie (Figure 11, page suivante).

Avant d'enregistrer notre fonte, nous allons lui donner un nom par l'intermédiaire du menu ***Éléments > Infos fonte***.

Avant de la générer, il est possible de réaliser une vérification automatique par le validateur de FontForge. Il exécute une série de tests et vérifie la fonte en entier. Il est accessible par le menu

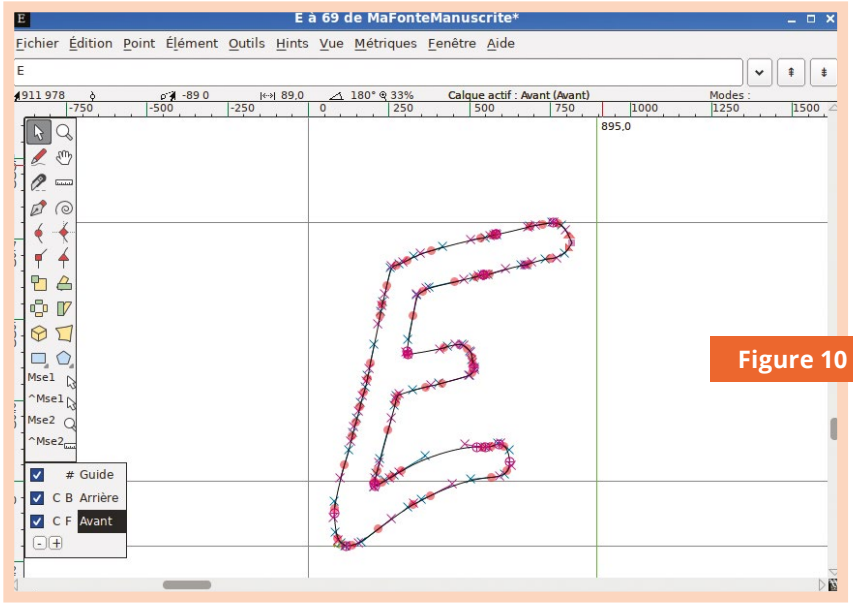
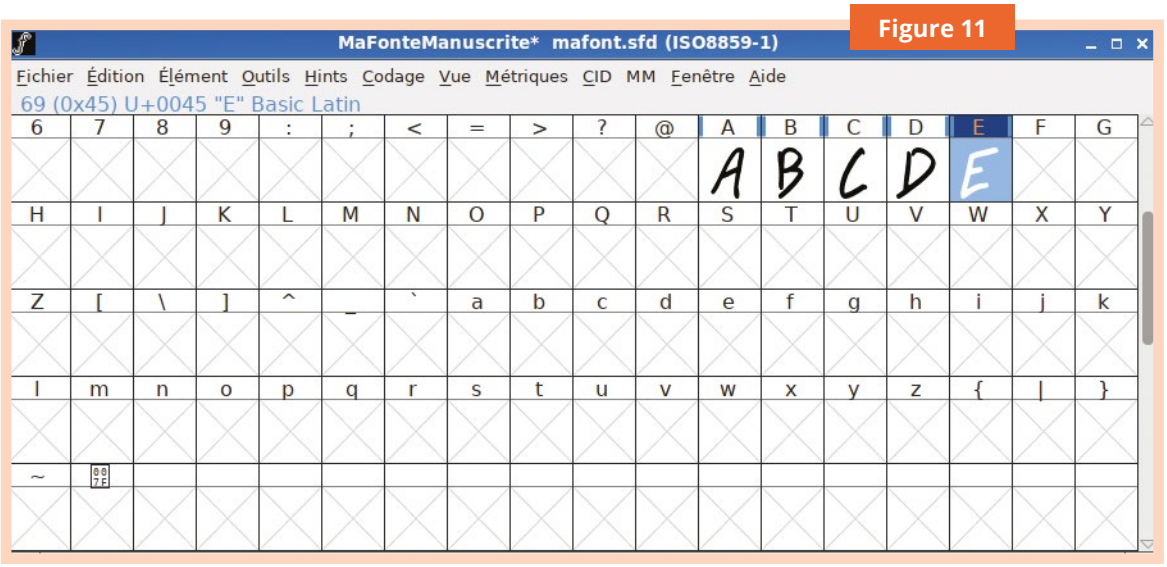

E à 69 de MaFonteManuscrite*
Fichier Édition Point Élément Outils Hints Vue Métriques Fenêtre Aide
Calque actif : Avant (Avant)
Modes :
Guide
C B Arrière
C F Avant

Figure 10

Figure 11

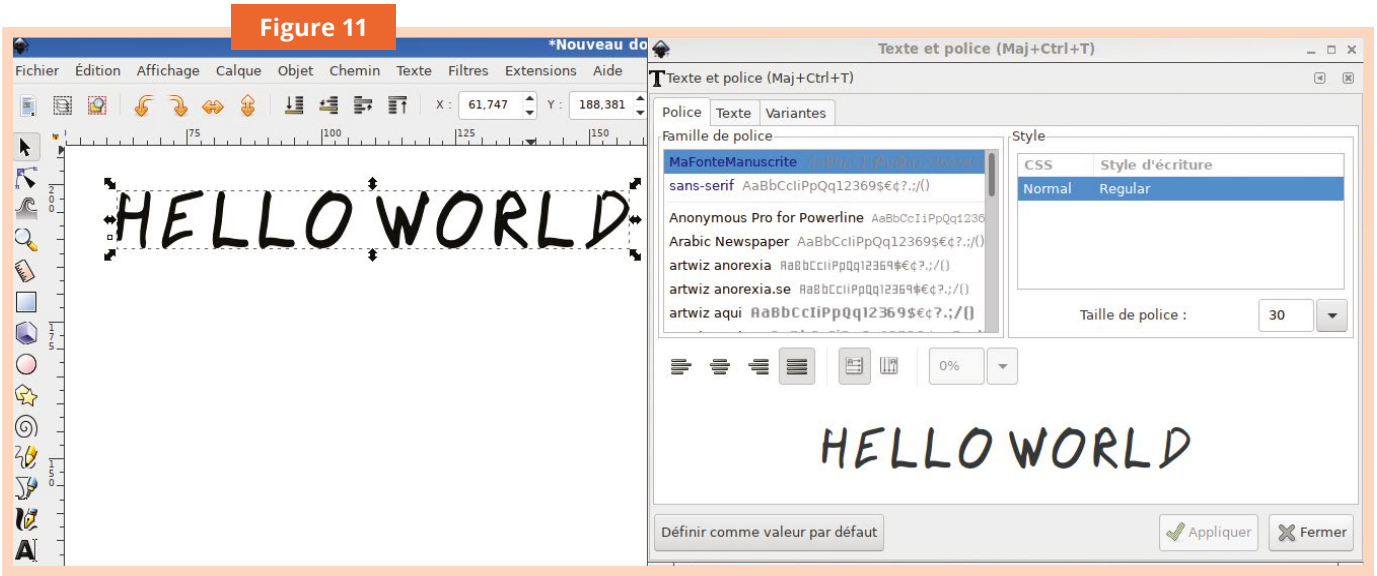

MaFonteManuscrite* mafont.sfd (ISO8859-1)
Fichier Édition Élément Outils Hints Codage Vue Métriques CID MM Fenêtre Aide
69 (0x45) U+0045 "E" Basic Latin

Élément > Validation. Le validateur est conçu pour exécuter uniquement les tests qui examinent la police pour l'exactitude technique. Dans mon cas, de nombreux problèmes subsistent. Lorsque le validateur termine son analyse, la fenêtre ***Validation*** s'ouvre et répertorie tous les problèmes trouvés par le validateur, présentés dans une liste triée par glyphe. Si vous double-cliquez sur un élément de la liste, FontForge ouvre le glyphe correspondant et met en évidence le(s) problème(s). La plupart du temps, on peut les éliminer rapidement en cliquant sur le bouton ***Corriger***.

Finalement, on génère la fonte à l'aide du menu ***Fichier > Générer fonte*** ou le raccourci [Shift]+[Ctrl]+[G]. Comme dans le cas de la modification de fonte, j'ai choisi le format *True Type Font* (TTF).

On clique sur le bouton ***Générer*** pour produire le fichier MaFonteManuscrite.ttf. On le copie ensuite dans le répertoire ~/.local/share/fonts et on relance fc-cache pour mettre à jour la liste des fontes disponibles :

Figure 11



```
$ cp MaFonteManuscrite.ttf ~/.local/share/
fonts
$ fc-cache -f -v
```

Nous pouvons maintenant tester notre fonte manuscrite dans Inkscape (Figure 12).

Voilà, il ne vous reste plus qu'à ajouter tous les glyphes afin de remplir la table : lettres minuscules, accentuées, chiffres et ponctuation. Ce travail est assez fastidieux et répétitif, je vous laisse le terminer tout seul ;-)

CONCLUSION

Nous avons terminé ce petit tutoriel de mise en œuvre de FontForge pour la modification et la création de fontes pour vos documents. Cet outil est très complet et vous permettra de modifier des fontes existantes assez rapidement. La création d'une fonte demande quant à elle un travail bien plus conséquent et surtout très répétitif. Il faudra vous armer de courage…

Dans cet article, nous n'avons fait qu'effleurer les fonctionnalités de FontForge sur ces deux exemples. Pour une maîtrise complète du logiciel, je vous renvoie vers la documentation **[5]**, notamment pour le design de fontes et le dessin de glyphes directement à partir de la fenêtre de glyphe. ■

RÉFÉRENCES

[1] http://caracteres.typographie.org/description/general.html

[2] https://fontforge.github.io/en-US/

[3] http://fontforge.github.io/en-US/documentation/interface/

[4] https://fr.wikipedia.org/wiki/Table_des_caractères_Unicode_%280000-0FFF%29

[5] http://designwithfontforge.com/fr-FR/

VOUS L'AVEZ RATÉ ?
VOUS AVEZ UNE DEUXIÈME CHANCE !

GNU/LINUX MAGAZINE
HORS-SÉRIE n°98

GNU LINUX MAGAZINE / FRANCE
SEPT. OCT. 2018
NOUVELLE FORMULE !
ACTUS
Les Dataclass : gros plan sur l'une des grandes nouveautés de Python 3.7
HORS-SÉRIE N°98
DÉCOUVERTE
Docker et les autres systèmes : qu'est-ce qu'un conteneur et à quoi cela sert-il ?
DOCKER
Comment installer, exécuter et créer des conteneurs
COMPRENEZ ENFIN TOUT SUR…
LES CONTENEURS !
POURQUOI ? QUAND ? COMMENT ?
ADMINISTRATION
La solution pour faciliter le déploiement des conteneurs : l'orchestration
KUBERNETES
Découvrez cet outil incontournable d'orchestration de Docker
INTERVIEW
Rencontre avec Adrien Duermael, développeur Docker

COMPRENEZ ENFIN TOUT SUR
LES CONTENEURS

À NOUVEAU DISPONIBLE

CHEZ VOTRE MARCHAND DE JOURNAUX ET SUR :
https://www.ed-diamond.com

RÉALISER UNE SAUVEGARDE ET LA RESTAURER avec Btrfs

PIERRE-ALAIN TORET

DISPONIBLE DEPUIS MAINTENANT PRESQUE 10 ANS, BTRFS EST UN SYSTÈME DE FICHIERS MATURE QUI EST POUSSÉ PAR SUSE, IL EST DEVENU LE SYSTÈME DE FICHIERS PAR DÉFAUT LORS DE SON INSTALLATION. IL OFFRE DES POSSIBILITÉS INTÉRESSANTES PAR RAPPORT AUX SYSTÈMES DE FICHIERS HISTORIQUES. DÉMONSTRATION AVEC UNE SAUVEGARDE/RESTAURATION À L'AIDE DE LA FONCTIONNALITÉ D'INSTANTANÉ (SNAPSHOT).

Le but de cet article n'est pas de présenter en détail le fonctionnement de Btrfs, mais de mettre en pratique l'une de ses fonctionnalités pour réaliser une sauvegarde de ses données et pour les restaurer si nécessaire.

Le tutoriel propose trois approches, une partie pour les sauvegardes locales, sur un disque physique différent, une partie sur les sauvegardes à distance, et une dernière partie qui permet de réaliser les sauvegardes sur d'autres systèmes de fichiers, déjà existants.

1. RAPPEL SUR LES SOUS-VOLUMES

Les sous-volumes sont une spécificité de Btrfs. Ce n'est en fait qu'une partie du système de fichiers ayant sa propre arborescence de fichiers. Le sous-volume peut-être accédé comme un dossier standard, ou en état monté à l'aide de l'option `subvol` de la commande `mount`. Il peut également être déplacé ou renommé comme un dossier et peut contenir un autre sous-volume dans sa sous-arborescence. Pour chaque partition Btrfs, il y a un sous-volume par défaut auquel l'id `5` est assigné et qui se nomme `/`. Celui-ci ne peut pas être modifié. C'est ce sous-volume qui est monté lorsqu'on ne précise rien.

PRÉ-REQUIS

Les prérequis ne sont pas nombreux. Dans les deux premières parties, il est simplement nécessaire d'avoir une partition Btrfs à disposition, ou à défaut, avoir de l'espace pour en créer une.

Une fois la partition créée, il faut d'abord la formater à l'aide de la commande suivante :

```
$ sudo mkfs.btrfs /dev/vdb1
```

Attention : Dans mon cas la partition est /dev/sdb1**, il est probable voire certain que ce n'est pas le cas sur votre machine. Vérifiez plusieurs fois que vous formatez la bonne partition avant de valider la commande.**

Dans notre cas, nous allons donc commencer par monter notre nouvelle partition dans /mnt :

```
$ sudo mkdir /mnt/btrfs
$ sudo mount /dev/vdb1 /mnt/btrfs
```

On peut constater qu'effectivement le sous-volume avec l'id 5 est celui monté.

```
$ sudo mount | grep vdb
/dev/vdb1 on /mnt/btrfs type btrfs
(rw,relatime,seclabel,space _
cache,subvolid=5,subvol=/)
```

Ensuite, nous allons créer un sous-volume et un fichier de test :

```
$ sudo touch /mnt/btrfs/test
$ sudo btrfs subvolume create /mnt/btrfs/sv1
Create subvolume '/mnt/btrfs/sv1'
$ sudo touch /mnt/btrfs/sv1/test _ sv1
```

Nous pouvons désormais constater que la partition contient notre fichier de test et ce qui apparaît comme un dossier (en réalité, notre sous-volume).

```
$  ls -lR /mnt/btrfs
/mnt/btrfs:
total 0
drwxr-xr-x. 1 root root 30 Mar  4 21:33 sv1
-rw-r--r--. 1 root root  0 Mar  4 21:23 test
/mnt/btrfs/sv1:
total 0
-rw-r--r--. 1 root root 0 Mar  4 21:33 test _
sv1
```

Démontons le sous-volume par défaut et remontons sv1 pour constater que nous voyons uniquement le contenu de celui-ci et non plus le contenu de toute la partition (l'option subvol est utilisée pour cela).

```
$ sudo umount /mnt/btrfs && sudo mount -o
subvol=sv1 /dev/vdb1 /mnt/btrfs
$ ls -lR /mnt/btrfs
/mnt/btrfs:
total 0
-rw-r--r--. 1 root root 0 Mar  4 21:33 test _ sv1
```

2. RAPPEL SUR LES INSTANTANÉS

Un instantané ou « snapshot » est un type de sous-volume Btrfs dont le contenu est initialisé à partir d'un sous-volume existant. Il est possible d'en créer en lecture-écriture ou en lecture seule (ce que nous utiliserons plus tard pour les sauvegardes).

Créons un nouveau sous-volume, nommons-le documents.

```
$ sudo btrfs subvolume create /mnt/btrfs/documents
Create subvolume '/mnt/btrfs/documents'
$ sudo chown ptoret: /mnt/btrfs/documents
```

J'ajoute deux fichiers et je crée un instantané à partir de documents qui s'appellera documents-snap.

```
$ ls -l /mnt/btrfs/documents
total 3170304
-rw-r--r-- 1 ptoret users 3122659328 Mar 16 18:12
Fedora-Server-dvd-x86 _ 64-29-1.2.iso
-rw-r--r-- 1 ptoret users  123731968 Mar 16 18:12
openSUSE-Leap-15.0-NET-x86 _ 64.iso
$ sudo btrfs subvolume snapshot /mnt/btrfs/
documents /mnt/btrfs/documents-snap
Create a snapshot of '/mnt/btrfs/documents' in
'/mnt/btrfs/documents-snap'
```

Supprimons un des fichiers et ajoutons-en un nouveau dans le sous-volume d'origine et listons le contenu des deux sous-volumes pour comparer.

```
$ ls -lR /mnt/btrfs/documents*
/mnt/btrfs/documents:
total 3049476
-rw-r--r-- 1 ptoret users 3122659328 Mar 16
18:12 Fedora-Server-dvd-x86 _ 64-29-1.2.iso
-rw-r--r-- 1 ptoret users         59 Mar 16
18:19 nouveau _ document.txt
```

```
/mnt/btrfs/documents-snap:
total 3170304
-rw-r--r-- 1 ptoret users 3122659328 Mar 16
18:12 Fedora-Server-dvd-x86 _ 64-29-1.2.iso
-rw-r--r-- 1 ptoret users  123731968 Mar 16
18:12 openSUSE-Leap-15.0-NET-x86 _ 64.iso
```

L'instantané contient bien le contenu d'origine alors que le répertoire contient lui le résultat des modifications effectuées (nouveau fichier et fichier supprimé).

» ATTENTION !
Un instantané ne fait en aucun cas office de sauvegarde.

3. LA SAUVEGARDE LOCALE

Une fois ces rappels faits, nous pouvons aborder la partie sauvegarde proprement dite. Nous allons utiliser ces deux notions, dans le cadre d'une sauvegarde locale, c'est-à-dire sur un support physiquement différent, mais présent sur la machine, dans notre cas un disque dur. Il est sous-entendu ici que le support physique a été partitionné en Btrfs.

» ATTENTION !
Une notion importante est l'imbrication des sous-volumes : lorsqu'on réalise un instantané sur un sous-volume, le contenu de l'instantané ne prend pas en compte les sous-volumes imbriqués dans le sous-volume d'origine. Attention donc si votre sous-volume en contient d'autres, ils ne seront pas pris en compte dans l'instantané réalisé, vous trouverez uniquement un dossier vide ayant le nom du sous-volume.

Tout d'abord, nous devons créer un instantané de type lecture seule.

```
$ sudo btrfs subvolume snapshot -r
/mnt/btrfs/documents /mnt/btrfsdocuments-
snap-ro
Create a readonly snapshot of '/mnt/
btrfs/documents' in '/mnt/btrfs/documents-
snap-ro'
```

Nous allons ensuite « envoyer » ce snapshot sur la partition Btrfs de la clef USB (dans notre cas /dev/vdc1). La partition où l'on va sauvegarder (la clef USB) est montée dans /mnt/usb.

```
$ sudo mount /dev/vdc1 /mnt/usb
$ sudo btrfs send /mnt/btrfs/documents-
snap-ro | sudo btrfs receive /mnt/usb/
$ ls -l /mnt/usb/documents-snap-ro/
total 3049476
-rw-r--r-- 1 ptoret users 3122659328 Mar 16
18:12 Fedora-Server-dvd-x86 _ 64-29-1.2.iso
-rw-r--r-- 1 ptoret users          59 Mar 16
18:19 nouveau _ document.txt
```

La commande btrfs send permet d'envoyer un sous-volume (en lecture seule) et la commande btrfs receive permet de l'écrire. Comme on le voit, il est très facile de copier un sous-volume (et donc tout son contenu à l'identique) d'un support physique à un autre. Le fait d'utiliser un pipe entre les deux commandes permet une très grande souplesse dans l'utilisation. On le verra lors de la sauvegarde à distance et sur un système de fichiers différent.

Il arrive que l'on dispose d'un disque déjà partitionné avec un autre système de fichiers que Btrfs, dans ce cas-là, l'option -f de l'utilitaire btrfs send est prévue pour spécifier un fichier de sortie au lieu d'envoyer sur la sortie standard. Le seul problème est que dans ce cas il n'est pas possible de parcourir le contenu de l'instantané.

```
$  sudo btrfs send -f /mnt/autrefs/
documents-snap-ro.btrfs documents-snap-ro
$ ls -l /mnt/autrefs/documents-snap-ro.
btrfs
total 3053528
-rw------- 1 root root 3126790515 Mar 16
22:01 documents-snap-ro.btrfs
drwx------ 2 root root      16384 Mar 16
21:59 lost+found
```

4. LA SAUVEGARDE INCRÉMENTALE

Lorsqu'on sauvegarde de grosses quantités de données et qu'une sauvegarde a déjà été réalisée, il peut être intéressant d'utiliser la fonctionnalité d'envoi incrémental proposée par btrfs send grâce à l'option -P. Dans mon cas, je rajoute une nouvelle ISO et je décide de sauvegarder à nouveau. En ayant gardé l'instantané précédent, je peux réaliser l'opération suivante, transférer le nouvel instantané (documents-snap-ro2) en référençant documents-snap-ro comme son parent, ainsi ce sera uniquement un différentiel entre ces deux versions qui sera envoyé.

```
$ sudo btrfs subvolume snapshot -r /mnt/
btrfs/documents /mnt/btrfs/documents-
snap-ro2
$ sudo btrfs send -p /mnt/btrfs/documents-
snap-ro /mnt/btrfs/documents-snap-ro2 |
sudo btrfs receive /mnt/usb/
```

On pourra ensuite supprimer documents-snap-ro dans /mnt/btrfs (côté disque de sauvegarde on peut le supprimer ou non, selon ce qu'on veut garder), car lors du prochain transfert on créera par exemple documents-snap3 et on prendra documents-snap-ro2 comme référence à passer via l'option -p.

```
$ sudo btrfs subvolume delete -c /mnt/
btrfs/documents/snap-ro
$ sudo btrfs subvolume snapshot -r /mnt/
btrfs/documents /mnt/btrfs/documents-
snap-ro3
$ sudo btrfs send -p /mnt/btrfs/documents-
snap-ro2 /mnt/btrfs/documents-snap-ro2 |
sudo btrfs receive /mnt/usb/
```

Dans le cas d'une sauvegarde sur un autre système de fichiers on peut également utiliser cette fonctionnalité. Mais je ne rentrerai pas plus dans les détails.

```
$ ls -lh /mnt/vieuxfs/
total 3.1G
-rw------- 1 root root 119M Mar 16 22:30
documents-snap-ro2.btrfs
-rw------- 1 root root 3.0G Mar 16 22:01
documents-snap-ro.btrfs
drwx------ 2 root root  16K Mar 16 21:59
lost+found
```

Comme on peut le voir, il n'est pas si aisé de s'y retrouver entre les instantanés qu'on crée côté système de fichiers à sauvegarder et ceux qui sont sur le support de sauvegarde. Il est intéressant d'utiliser des outils pour automatiser tout cela.

5. LA SAUVEGARDE À DISTANCE

La sauvegarde à distance ne présente pas plus de difficulté, il suffira d'utiliser ssh pour réaliser l'envoi-réception à l'aide des outils Btrfs. Ainsi, si l'on désire envoyer le dernier instantané, on peut utiliser la commande suivante (l'option -p pourra également être utilisée, moyennant l'envoi d'un premier instantané qui servira ensuite de référence). Il arrivera dans /mnt/usb sur la machine distante (sous réserve que /mt/usb abrite bien une partition Btrfs).

```
$ sudo btrfs send /mnt/btrfs/documents-
snap-ro  | ssh ptoret@192.168.122.102 sudo
btrfs receive /mnt/usb/
At subvol /mnt/btrfs/documents-snap-ro
```

6. CHIFFRER ET/OU COMPRESSER SA SAUVEGARDE

Le fait d'utiliser un « pipe » UNIX (connu aussi sous le nom de tube) permet de nombreuses choses, comme compresser les sauvegardes sur le support externe par exemple. Un autre avantage est de pouvoir chiffrer celles-ci, surtout dans le cas où on les entreposerait sur un serveur en ligne par exemple. Pour réaliser ceci, il faut une clef publique et utiliser celle-ci de la façon suivante (on chiffre pour Alice qui est le destinataire dans l'exemple, dans les faits, on sera probablement le possesseur de la clef privée aussi, il faut bien pouvoir déchiffrer sa propre sauvegarde).

```
$ sudo btrfs send /mnt/btrfs/documents-snap-ro  |
gpg -e -r alice@tld > documents-snap-ro.gpg
```

On peut également chiffrer après avoir compressé de la façon suivante :

```
$ sudo btrfs send /mnt/btrfs/documents-
snap-ro  | pigz - | gpg -e -r alice@tld >
documents-snap-ro.gz.gpg
```

Ces deux exemples sont à adapter à vos cas d'usage, mais donne un exemple de ce qu'il est possible de faire, le plus simple est de parcourir les pages de manuels des différents outils pour se donner une idée des possibilités. À noter que selon la taille du sous-volume à compresser, cela peut prendre un temps considérable.

7. RESTAURER SA SAUVEGARDE

Réaliser des sauvegardes est une bonne chose, savoir accéder à ses données sauvegardées en cas de problème est encore mieux.

On peut imaginer plusieurs cas de figure auxquels je vais essayer de proposer une solution.

Cas 1 : « j'ai supprimé un fichier et je veux le restaurer depuis la sauvegarde »

Dans le cas où la sauvegarde est sur un système de fichiers Btrfs, elle peut se parcourir comme un dossier, ce qui rend très facile la récupération d'un fichier supprimé.

Ainsi, si je reprends le tout premier exemple, après avoir créé l'instantané documents-snap, j'ai supprimé le fichier openSUSE-Leap-15.0-NET-x86_64.iso. Pour le récupérer, je pourrais simplement le copier à son emplacement initial depuis l'instantané.

```
$ cp /mnt/btrfs/documents-snap-ro/openSUSE-Leap-15.0-NET-x86 _ 64.
iso /mnt/btrfs/documents/openSUSE-Leap-15.0-NET-x86 _ 64.iso
```

Dans le cas d'une sauvegarde distante, cela donnerait :

```
$ scp ptoret@192.168.122.102:/mnt/usb/documents-snap-ro/
openSUSE-Leap-15.0-NET-x86 _ 64.iso /mnt/btrfs/documents/
openSUSE-Leap-15.0-NET-x86 _ 64.iso
```

» ATTENTION !
Il n'est pas possible de restaurer un fichier de façon si simple lorsque la sauvegarde est réalisée sur un système de fichiers autre que Btrfs. Il faudrait alors restaurer tout le sous-volume comme dans le cas 2 et une fois cela fait, revenir au cas 1 pour récupérer le fichier manquant.

Cas 2 : « je veux restaurer tout mon sous-volume »

Ici, on peut imaginer le cas d'un disque qui est tombé en panne ou autre ne laissant plus aucune trace du sous-volume d'origine.

Dans ce cas-là, il faut 2 étapes.

Récupérer le sous-volume sur le système de fichiers local.

Dans le cas où la sauvegarde est à distance :

```
$ ssh ptoret@192.168.122.102 sudo btrfs send /mnt/usb/
documents-snap-ro | sudo btrfs receive /mnt/btrfs/
At subvol /mnt/usb/documents-snap-ro
```

Dans le cas où la sauvegarde est locale :

```
$ sudo btrfs send /mnt/usb/documents-snap-ro  | sudo btrfs
receive /mnt/btrfs
At subvol /mnt/btrfs/documents-snap-ro
```

Repasser le sous-volume en lecture/écriture.

```
$ sudo btrfs property set -tsubvol /mnt/btrfs/documents-
snap-ro ro false
```

Enfin, il suffit de renommer le sous-volume :

```
$ sudo mv /mnt/btrfs/documents-snap-ro /mnt/btrfs/documents
```

» ATTENTION !
Suivre cet article devrait vous permettre d'avoir une bonne idée de ce qu'il est possible de faire, mais il est important de tester sa propre procédure de restauration au calme, juste pour être sûr de pouvoir le faire le jour où un problème survient (on se retrouve souvent un peu paniqué dans ces moments-là).

ALLER PLUS LOIN

La gestion des instantanés que ce soit en local ou à distance peut vite devenir complexe, il est possible d'écrire des scripts pour automatiser, à vrai dire un simple cron peut suffire, mais il existe également de nombreux outils qui peuvent s'occuper de cela pour vous.

Il est possible d'obtenir un fonctionnement type « time-machine » **[1]**. Une solution générique a d'ailleurs été proposée sous le nom d'autosnap **[2]**, mais elle n'est pas encore disponible dans les distributions.

Actuellement, l'outil le plus connu est sans doute Snapper **[3]** qui est développé par SUSE (mais utilisable sur de nombreuses distributions), il mériterait un article à lui seul, car il est très complet et possède de nombreux plugins. Il est néanmoins nécessaire d'adopter un agencement particulier des instantanés pour que ce dernier fonctionne.

Pour les sauvegardes, un outil relativement répandu est btrbk **[4]**. Il permet de mettre en place assez facilement une sauvegarde dans le cadre d'un PC portable et d'un disque dur externe par exemple. ■

RÉFÉRENCES

[1] https://btrfs.wiki.kernel.org/index.php/UseCases#How_can_I_use_btrfs_for_backups.2Ftime-machine.3F

[2] https://btrfs.wiki.kernel.org/index.php/Autosnap

[3] https://github.com/openSUSE/snapper

[4] https://github.com/digint/btrbk

ACTUELLEMENT DISPONIBLE !

GNU/LINUX MAGAZINE n°228

GNU LINUX MAGAZINE / FRANCE
DÉVELOPPEMENT ET ADMINISTRATION SUR SYSTÈMES UNIX & OPEN SOURCE
N°228
JUILLET AOÛT 2019
Actus / Quantum Computing
SIMULEZ UN ORDINATEUR QUANTIQUE p.12
DÉCOUVREZ LES FONDEMENTS DE LA LOGIQUE QUANTIQUE
RÉALISEZ VOTRE TOUT PREMIER PROGRAMME QUANTIQUE ET EXÉCUTEZ-LE !
DevOps / Conteneurs
DÉPLOYEZ SIMPLEMENT DES APPLICATIONS COMPLEXES GRÂCE AUX OPÉRATEURS KUBERNETES p.42
Signaux / C
TOUT SAVOIR SUR LA GESTION DES TIMERS EN C p.50
Sécurité / Shell
RÉALISEZ UN VPN « MAISON » À PARTIR DE TOR ET QUELQUES OUTILS OPEN SOURCE p.68
SDR / Reed-Solomon
CODAGE D'INFORMATIONS PAR BLOCS : LA CORRECTION D'ERREURS DE TRANSMISSION p.28
Conférence / Kubernetes
RÉTROSPECTIVE SUR LA KUBECON EUROPE 2019 p.06
ET AUSSI... DÉVELOPPEMENT EMBARQUÉ AVEC MICROPYTHON

SIMULEZ UN ORDINATEUR QUANTIQUE

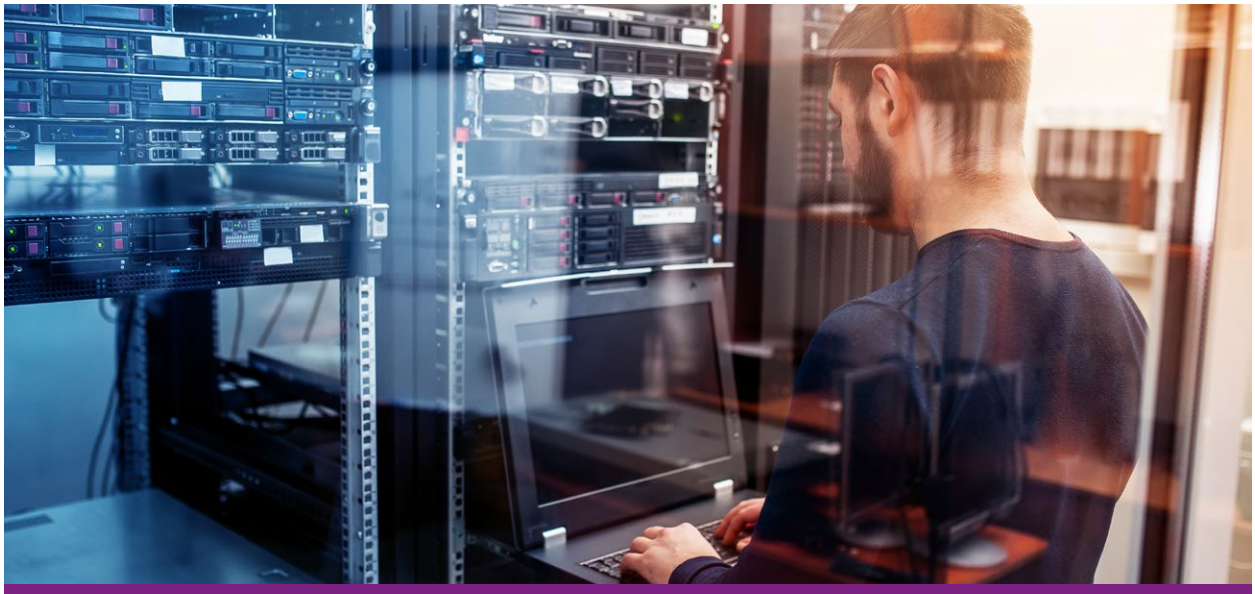
NE LE MANQUEZ PAS
CHEZ VOTRE MARCHAND DE JOURNAUX ET SUR :
https://www.ed-diamond.com

Installer, configurer et sécuriser un SERVEUR APACHE2

MICHAËL BERTOCCHI

Outil utilisé : Apache 2 - **Site du projet :** https://httpd.apache.org/

APACHE EST UN SERVEUR WEB : TOUT COMME TOMCAT ET NGINX, IL PERMET DE SERVIR DES PAGES WEB AUX INTERNAUTES. APRÈS L'AVOIR INSTALLÉ, NOUS DÉCOUVRIRONS LES PRINCIPAUX FICHIERS DE CONFIGURATION ET COMMANDES À CONNAÎTRE, APPRÉCIERONS L'USAGE DES VIRTUALHOSTS ET ENFIN, NOUS RAPPELLERONS COMMENT SÉCURISER AU MIEUX NOTRE SERVEUR WEB.



ÉTAPE 1

INSTALLONS LE SERVEUR WEB APACHE

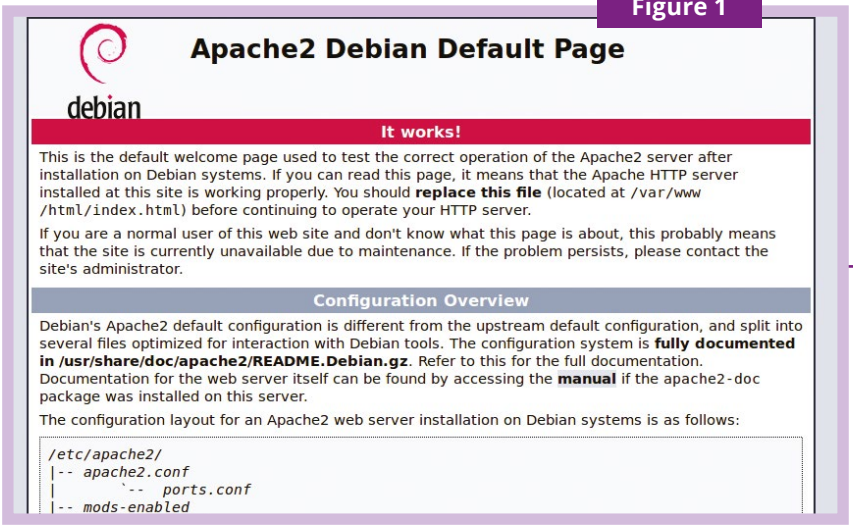
Utilisant une distribution Debian 9 dans cet article, nous utiliserons la commande apt-get :

```
apt-get install apache2
```

Une fois installé, en ouvrant votre navigateur, vous verrez la page illustrée en Figure 1.

C'est une simple page web HTML, mais où est ce fichier me demanderez-vous ? Pour le trouver, il faut vous rendre dans le répertoire de configuration des « virtualhosts » :

Figure 1


Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled

```
vi /etc/apache2/sites-enabled/000-default.conf
```

Vous y verrez un fichier se présentant ainsi :

```
<VirtualHost *:80>
        # The ServerName directive sets the
request scheme, hostname and port that
        # (...)
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
```

Notez ici la directive DocumentRoot qui indique le répertoire racine du site virtuel, vous y trouverez un simple fichier HTML index.html. Mais nous verrons ceci plus en détail plus tard.

ÉTAPE 2

AJOUTONS LE SUPPORT PHP

En l'état, vous ne pouvez écrire que des pages HTML, il serait plus intéressant de faire des pages dynamiques avec par exemple du php, pour cela, nous pouvons installer le module associé via apt-get :

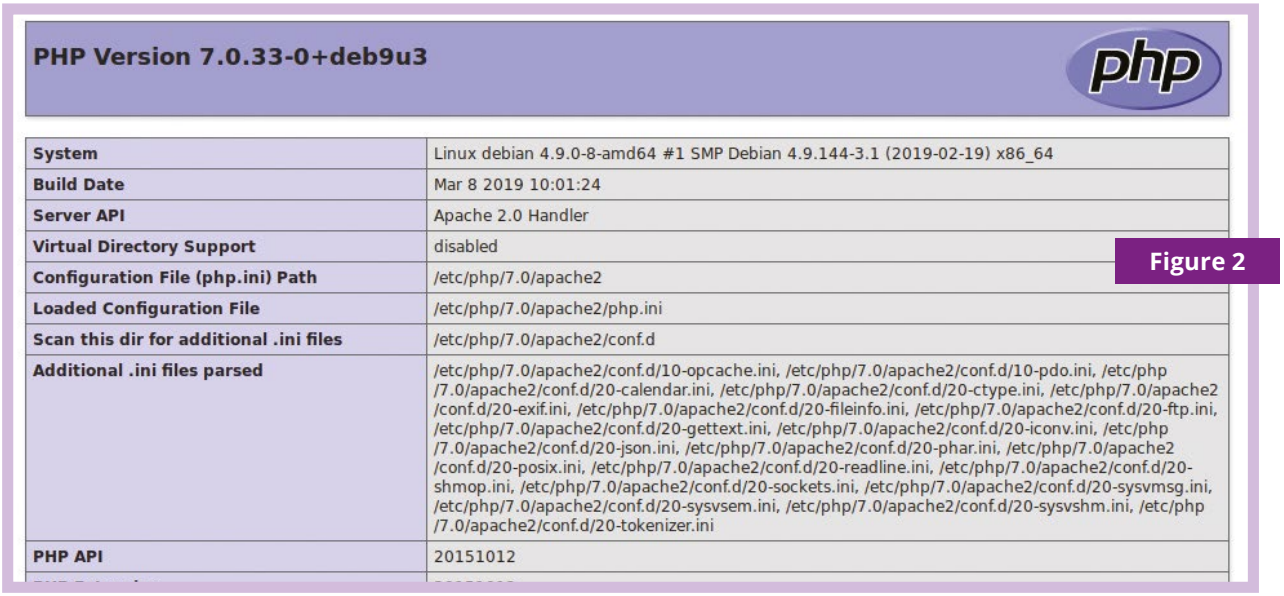
```
apt-get install libapache2-mod-php
```

Ajoutons un premier fichier php pour vérifier la bonne installation du module :

```
echo "<?php phpinfo();" > /var/www/html/info.php
```

En ouvrant votre navigateur à l'adresse **http://localhost/info.php**, vous pourrez confirmer le bon fonctionnement (Figure 2).

Figure 2



ÉTAPE 3

OBSERVONS LA CONFIGURATION

Sur les distributions Debian, les fichiers de configuration sont centralisés dans l'arborescence /etc/application.

Dans notre cas, il faut observer les arborescences /etc/apache2 et /etc/php/7.0.

Commençons par apache :

```
root@debian:/etc/apache2# ls -1
apache2.conf
conf-available
conf-enabled
envvars
magic
mods-available
mods-enabled
ports.conf
sites-available
sites-enabled
```

Ici, les répertoires qui nous intéressent sont :

- conf-available/ : quelques configurations (charset, sécurité…) ;
- mods-available/ : la configuration des modules ;
- sites-available/ : les fichiers virtualhosts.

ainsi que les fichiers :

- apache2.conf : le fichier principal de configuration ;
- ports.conf : comme l'indique son nom, le/les ports à écouter.

En éditant le fichier apache2.conf, vous comprendrez la philosophie générale de configuration : certains paramètres sont présents dans ce fichier, mais le reste est dispatché.

```
# It is split into several files forming
the configuration hierarchy outlined
# below, all located in the /etc/apache2/
directory:
#
#       /etc/apache2/
#       |-- apache2.conf
#       |       `--  ports.conf
#       |-- mods-enabled
#       |       |-- *.load
#       |       `-- *.conf
#       |-- conf-enabled
#       |       `-- *.conf
#       `-- sites-enabled
#               `-- *.conf
```

Ensuite, vous remarquerez des doublons dans les répertoires, en effet on a d'un côté les fichiers dans les répertoires terminant par -available et dans ceux terminant par -enabled, des liens symboliques vers ceux-ci. En effet, vous avez des commandes qui le permettent :

- a2ensite / a2dissite : pour activer/désactiver un virtualhost ;
- a2enconf / a2disconf : pour activer/désactiver un fichier de configuration ;
- et a2enmod / a2dismod : pour activer/désactiver un module.

Comme dit précédemment, leur seule action est de créer/supprimer un lien symbolique entre les deux répertoires.

C'est la même chose pour /etc/php/7.0 :

```
root@debian:/etc/php/7.0# ls -1
apache2
cli
mods-available
```

Notez une différence : pour php, vous pouvez différencier les fichiers de configuration des pages web php /etc/php/7.0/apache2 et des batchs/scripts php /etc/php/7.0/cli.

Par exemple, une page web php doit avoir un temps d'exécution

limité pour éviter que l'internaute attende plusieurs minutes en cas de boucle infinie, en revanche il est courant d'avoir des scripts/batchs qui durent plusieurs minutes, idem pour les modules qui peuvent être différents, la gestion d'erreurs…

ÉTAPE 4

UTILISONS LA PUISSANCE DES VIRTUALHOSTS

Les virtualhosts ou « hôtes virtuels » permettent de paramétrer plusieurs sites web sur le même serveur. N'ayant pas de serveur DNS à disposition, nous utiliserons notre fichier hosts pour simuler ces différentes entrées.

Éditez le fichier /etc/hosts pour ajouter deux entrées site.fraise.local et site.poire.local :

```
vi /etc/hosts
```

```
127.0.0.1       localhost site.fraise.local
site.poire.local
```

Pour rappel, lorsque vous tapez un nom de domaine dans votre navigateur, le système doit convertir celui-ci en IP pour savoir à quel serveur envoyer la requête. Dans les faits, il cherche d'abord dans le fichier hosts avant de demander au serveur DNS. En entrant ces deux noms, votre navigateur interrogera votre PC (127.0.0.1, tout comme localhost étant votre adresse de PC locale).

Désormais, il nous reste plus qu'à créer deux fichiers de virtualhosts pour ces deux adresses.

Créez simplement :

```
vi /etc/apache2/sites-available/site.fraise.
local.conf
```

```
<VirtualHost *:80>
        ServerName site.fraise.local

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/fraise/

        ErrorLog ${APACHE _ LOG _ DIR}/
fraise-error.log
        CustomLog ${APACHE _ LOG _ DIR}/
fraise-access.log combined

</VirtualHost>
```

Notez plusieurs points :

- ServerName : pour indiquer le nom de domaine de ce virtualhost ;
- DocumentRoot : le chemin vers le site où emmener l'internaute ;
- ErrorLog / CustomLog pour différencier les logs de vos différents sites (pratique pour investiguer).

Faites de même pour site.poire.local.conf.

Ensuite, activez-les via la commande a2ensite :

```
a2ensite site.fraise.local.conf
```

Le lien symbolique a bien été créé, il faut indiquer au service apache de prendre en compte cette nouvelle configuration via :

```
systemctl reload apache2
```

Si vous vous rendez à cette adresse, vous aurez une erreur, en effet, il faut créer le répertoire du site et y créer une page web, par exemple en html (mais cela pourrait être en php ou autre).

Figure 3

Figure 4

```
mkdir /var/www/html/fraise/
vi /var/www/html/fraise/index.htm
```

```
<html>
<head><title>Site fraise</title></head>
<body>
        <h1>Site fraise</h1>
</body>
</html>
```

Faites de même pour le site « poire » dans un autre répertoire et vous pourrez apprécier d'avoir deux sites sur le même serveur (voir Figures 3 et 4, page précédente).

ÉTAPE 5

SÉCURISONS NOTRE SERVEUR APACHE

La sécurité est trop souvent négligée aujourd'hui, or il suffit de quelques interventions sur votre configuration pour l'améliorer.

Il faut respecter plusieurs règles :

- cacher toute information concernant le système, service et leurs versions ;
- cacher les messages d'erreurs qui pourraient aider à comprendre la technologie / l'algorithme utilisés ;
- ne pas permettre l'encapsulation de votre site ;
- limiter le périmètre de visibilité de vos sources.

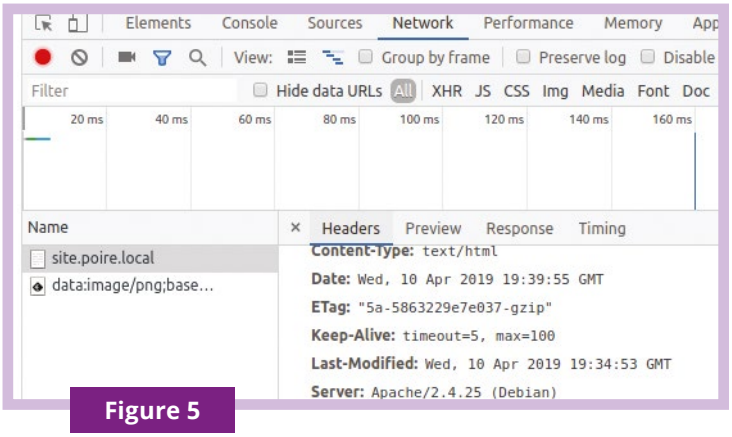


Figure 5

ÉTAPE 6

CACHONS CETTE VERSION QU'ILS NE SAURAIENT VOIR

En utilisant le plugin de développement sous votre navigateur ([F12] en général), vous pouvez vérifier si votre configuration est ou non verbeuse, par exemple, ici en analysant votre configuration par défaut vous pourrez voir la version du serveur apache ainsi que la distribution utilisée (voir figure 5).

Pour rendre votre instance plus discrète, il vous suffit d'éditer le fichier security :

```
vi /etc/apache2/conf-available/security.conf
```

et passer la directive ServerTokens à Prod et ServerSignature à Off :

```
#ServerTokens Minimal
#ServerTokens OS
#ServerTokens Full
ServerTokens Prod

ServerSignature Off
#ServerSignature On
```

Rechargez la configuration apache via l'habituel :

```
systemctl reload apache2
```

Faites ensuite un rafraîchissement de votre page, et vous aurez le plaisir de voir juste « Apache » au lieu de la version et la distribution.

ÉTAPE 9

DÉTERMINONS NOTRE RACINE WEB INTELLIGEMMENT

Si vous avez un site écrit en php par exemple, vous avez une arborescence plus ou moins complexe avec des répertoires que vous ne souhaitez pas exposer, par exemple les fichiers CSS, JavaScript… Lorsque l'on utilise des frameworks (comme Zend Framework, Laravel, Symfony, mkframework…), ceux-ci indiquent clairement ce fameux répertoire, aussi appelé « webroot » (racine web), et souvent donnent un exemple de virtualhost pour faciliter l'installation de son site web.

Imaginons une arborescence du type :

```
├── conf
├── domains
├── logs
├── models
└── public
    ├── css
    ├── index.php
    └── js
```

Vous êtes bien d'accord que vous ne souhaitez pas exposer vos répertoires conf/ et logs/ qui pourraient contenir des informations nuisibles. Pour cela, nous utilisons la racine web : DocumentRoot dans le virtualhost.

Dans notre exemple, le fichier serait ainsi :

```
<VirtualHost *:80>
        ServerName site.fraise.local

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/fraise/
public/

        ErrorLog ${APACHE _ LOG _ DIR}/
fraise-error.log
        CustomLog ${APACHE _ LOG _ DIR}/
fraise-access.log combined
</VirtualHost>
```

En faisant ainsi, l'internaute ne peut voir que le contenu du répertoire public/ (comme souhaité), il ne peut pas remonter d'un niveau (même en tapant ../).

CONCLUSION

Vous avez vu dans cet article comment installer, configurer votre serveur web apache. C'est un bon produit qui n'a cessé de s'améliorer avec le temps, notamment avec cette modularité de configuration avec la possibilité de préparer un fichier de configuration et de choisir de l'activer ou non. Cela permet également de faciliter un rollback éventuel en cas de soucis : en désactivant rapidement un fichier de configuration posant souci d'une simple commande pour regarder, analyser à tête reposée.

Vous avez également, je l'espère pu apprécier la force des virtualhosts qui permettent non seulement de configurer plusieurs sites sur un même serveur, ainsi que de configurer des déclinaisons avec des paramètres différents : par exemple, l'affichage des erreurs activé sur une URI de développement et désactivé sur celle de recette (ou de production bien entendu). ■

On pourrait donc ajouter une entrée dans votre fichier hosts avec ce virtualhost associé, on aurait donc en fonction de l'url l'affichage ou non des messages d'erreur, ceci en pointant sur les mêmes sources.

```
<VirtualHost *:80>
        ServerName dev.fraise.local

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/fraise/

        ErrorLog ${APACHE _ LOG _ DIR}/
fraise-error.log
        CustomLog ${APACHE _ LOG _ DIR}/
fraise-access.log combined

        php _ flag display _ errors On
</VirtualHost>
```

ÉTAPE 7

DÉSACTIVONS L'AFFICHAGE DES MESSAGES D'ERREURS TROP BAVARDS

Nous devons faire de même pour les erreurs php, il ne faut pas qu'apparaisse sur votre site une stacktrace indiquant une partie de votre code source.

Pour cela, vous devez éditer votre fichier de configuration php :

```
vi /etc/php/7.0/apache2/php.ini
```

Vérifiez que la directive display_errors est bien désactivée, et que log_errors est bien activée. Ainsi, les erreurs ne seront pas affichées au vu de tous, mais vous pourrez les consulter dans votre fichier de log (configuré précédemment dans le virtualhost : par exemple /var/log/apache2/fraise-error.log).

```
display _ errors = Off
log _ errors = On
```

Si vous souhaitez avoir l'affichage de vos erreurs, plutôt que de les activer sur le fichier de configuration globale, impactant tous vos sites, mieux vaut l'activer au cas par cas sur chaque virtualhost : vous pouvez par exemple avoir un virtualhost de développement avec les erreurs et l'autre de test/recette sans. Ceci grâce à la directive php_flag qui permet de surcharger votre configuration php uniquement pour ce site.

ÉTAPE 8

INTERDISONS L'ENCAPSULATION DE NOTRE SITE

Une mesure de sécurité peut être aussi de ne pas autoriser votre site à être inclus dans une frame/iframe, permettant à un hacker de faire du phishing.

Pour cela, il faut faire deux choses, dans un premier temps activer une directive en rééditant votre fichier security :

```
vi /etc/apache2/conf-available/security.conf
```

et activer la ligne commentée suivante :

```
Leader set X-Frame-Options: "sameorigin"
```

Mais pour cela, il faut faut activer le module associé :

```
a2enmod headers
```

Rechargez à nouveau votre configuration via la commande reload d'apache :

```
systemctl reload apache2
```

Et en rechargeant votre site, vous verrez apparaître une nouvelle ligne dans le plugin développeurs :

```
X-Frame-Options: sameorigin
```

ACTUELLEMENT DISPONIBLE

GNU/LINUX MAGAZINE HORS-SÉRIE N°103

GNU LINUX MAGAZINE / FRANCE
DÉVELOPPEMENT ET ADMINISTRATION SUR SYSTÈMES UNIX & OPEN SOURCE
HORS-SÉRIE N°103
JUILLET AOÛT 2019
FRANCE MÉTRO. : 14,90 €
CH : 23.80 CHF
PORT : 15,90 €
MAR : 165 MAD
DOM/S : 15,90 €
CAN : 23.99 $CAD
ÉMULATEURS
Développez sur microcontrôleur... sans microcontrôleur !
DÉVELOPPEZ DES
EXTENSIONS & PLUGINS
POUR AMÉLIORER VOS APPLICATIONS
LUA
JAVASCRIPT
PYTHON
CHROME/ FIREFOX
Développez des extensions pour vos navigateurs web en JavaScript
VLC
Créez des plugins pour votre lecteur multimédia grâce au langage Lua
LIBREOFFICE
Générez facilement des documents en pilotant LibreOffice en Python
INTERFACES GRAPHIQUES
Automatisez n'importe quelle tâche graphique pénible ou répétitive
BASE DE DONNÉES
Découvrez comment démarrer et utiliser un cluster de développement ScyllaDB
DÉVELOPPEMENT
Utilisez vos bibliothèques C dans vos programmes Go
L 15066 - 103 H - F: 14,90 € - RD

NE LE MANQUEZ PAS

CHEZ VOTRE MARCHAND DE JOURNAUX ET SUR :

https://www.ed-diamond.com

SÉCURISEZ LES SECRETS DE VOTRE INFRASTRUCTURE avec Ansible

ROMAIN PELISSE

UN PRÉCÉDENT ARTICLE A DÉJÀ PRÉSENTÉ EN DÉTAIL LE FONCTIONNEMENT ET L'UTILISATION DE ANSIBLE [1]. NOUS ALLONS DONC REPARTIR DE LÀ ET ALLER UN PEU PLUS LOIN EN ABORDANT LA PROBLÉMATIQUE, DIFFICILE ET SOUVENT COMPLEXE, DE LA GESTION DES SECRETS. COMME NOUS ALLONS LE VOIR, SI LE SUJET EST ARDU, ANSIBLE APPORTE TOUS LES ÉLÉMENTS NÉCESSAIRES POUR ASSURER LA CONFIDENTIALITÉ DES SECRETS LORS DE LEUR DÉPLOIEMENT. PETITE DÉMONSTRATION PAR LA PRATIQUE AVEC LA MISE EN PLACE D'UN SERVEUR VSFTP À L'AIDE DE ANSIBLE.

Nous allons commencer notre cas d'étude en mettant en place l'installation du serveur vsftpd à l'aide d'Ansible. L'article ayant décrit en détail la syntaxe et le fonctionnement de Ansible, nous n'allons pas expliciter en détail chaque aspect de cette installation, mais tout de même nous assurer que l'exemple présenté est fonctionnel (et pourra donc servir de point de départ au lecteur curieux).

1. MISE EN PLACE DU SERVEUR FTP

1.1 Qu'est-ce qu'un serveur FTP ?

À titre de rappel ou simplement pour le lecteur peu familier du sujet, FTP est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers ou depuis un autre ordinateur situé sur le même réseau (ou accessible depuis le réseau utilisé). Il permet aussi de supprimer ou même de modifier les fichiers ainsi partagés.

Comme il est dédié au partage de fichiers, il est beaucoup plus efficace que, par exemple, le protocole HTTP. Néanmoins, il n'est que rarement autorisé sur les sites accessibles sur Internet et son utilisation est donc souvent confinée à des réseaux privés.

Le protocole FTP suit le modèle « classique » du client-serveur. Il y a donc un logiciel « client », qui envoie des requêtes vers un logiciel « serveur », généralement désigné sous le nom de « serveur FTP ».

1.2 Installation

Cette première étape consiste à installer le paquetage associé au serveur vsftpd, ainsi que le paquetage associé au firewall. Ce dernier est probablement déjà installé, mais il est important d'indiquer la dépendance entre les deux, surtout que vsftpd est un serveur très sécurisé, donc il serait abscons de le déployer sans firewall :

```
---
- name: ftp server installed
  hosts: localhost
  gather_facts: no
  become: yes
  become_method: sudo
  tasks:
    - name: latest vsftpd version installed
      yum:
        name: vsftpd
        state: latest
    - name: latest firewalld version installed
      yum:
        name: firewalld
        state: latest
```

Attention, avant d'aller plus loin, commençons déjà par vérifier que tout ceci fonctionne et que la syntaxe du fichier est correcte :

```
$ sudo ansible-playbook vsftd.yml
[sudo] Mot de passe de rpelisse :
 [WARNING]: provided hosts list is empty, only localhost is
available. Note that the implicit localhost does not match 'all'


PLAY [ftp server installed] ****************************************
********************************************************************
********************************************************************

TASK [latest vsftpd version installed] *****************************
********************************************************************
********************************************************************
ok: [localhost]

TASK [latest firewalld version installed] **************************
********************************************************************
********************************************************************
ok: [localhost]

PLAY RECAP *********************************************************
********************************************************************
********************************************************************
localhost                  : ok=2    changed=0    unreachable=0
failed=0
```

Nous n'illustrons plus l'exécution d'Ansible dans le reste de l'article (pour rester succinct). Cela dit, lors de ses tests, il est fortement recommandé au lecteur d'exécuter Ansible à chaque changement dans le fichier de configuration, pour s'assurer, de manière incrémentale, du bon fonctionnement de la configuration.

1.3 Démarrage des services et ouverture de port

Nous allons maintenant nous assurer que les services nécessaires sont bien démarrés. Il nous faudra bien évidemment démarrer le serveur vsftd, mais aussi nous assurer, toujours dans un souci de sécurité, que le firewall est aussi démarré. Avec celui-ci en route, il est aussi important de ne pas oublier d'ouvrir le port dédié au protocole FTP :

```
- name: vsftpd is enabled and running
  service:
    name: vsftpd
    enabled: true
    state: started

- name: firewalld is enabled and running
  service:
    name: firewalld
    enabled: true
    state: started

- name: firewalld allows ftp
  firewalld:
    service: ftp
    permanent: true
    state: enabled
    immediate: yes
```

1.4 Tester le service mis en place

Une fois le script Ansible exécuté sans erreur, vérifions que le service est bien démarré :

```
$ sudo systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/
vsftpd.service; enabled; vendor preset:
disabled)
   Active: active (running) since Fri 2019-
05-17 09:09:11 CEST; 5 days ago
 Main PID: 1214 (vsftpd)
    Tasks: 1 (limit: 4915)
   Memory: 840.0K
   CGroup: /system.slice/vsftpd.service
           └─1214 /usr/sbin/vsftpd /etc/
vsftpd/vsftpd.conf

mai 17 09:09:11 localhost.localdomain
systemd[1]: Starting Vsftpd ftp daemon...
mai 17 09:09:11 localhost.localdomain
systemd[1]: Started Vsftpd ftp daemon.
```

Tout est en ordre ! Passons donc maintenant au sujet de cet article : la gestion de secrets avec Ansible.

2. GESTION DE SECRETS AVEC ANSIBLE

2.1 Création d'un compte utilisateur

Notre serveur FTP est en place, mais reste encore à y donner accès à nos utilisateurs. Nous allons donc demander à Ansible de créer pour nous les comptes utilisateurs à partir de liste fournie sous forme de variables. Définissons cette variable, dans un fichier à part nommé users.yml :

```
$ cat users.yml
ftp_users:
  - { username: mike, password: mike-mot-
de-passe }
  - { username: bob, password: bob-mot-de-
passe }
```

Modifions maintenant notre script Ansible pour y ajouter la création des comptes utilisateurs :

```
---
- name: ftp server installed
  hosts: localhost
  gather_facts: no
  become: yes
  become_method: sudo
  vars_files:
    - users.yml
  tasks:
...

    - name: "Create user accounts for the
FTP server"
      user:
        name: "{{ item.username }}"
        password: "{{ item.password }}"
      with_items: "{{ ftp_users }}"
```

Tout ceci est relativement trivial et se déroule donc sans difficulté. Lors de l'exécution du script, les comptes utilisateurs sont créés et accessibles à l'aide de leur mot de passe. Le problème réside ici justement dans la gestion de ces derniers.

Comme le lecteur n'aura pas manqué de le noter, les mots de passe sont spécifiés, en clair, dans le fichier users.yml. Ce qui signifie que n'importe quelle personne qui a accès à Ansible a donc accès à ces mots de passe. Ceci pose bien évidemment des risques inacceptables en termes de sécurité. Heureusement, Ansible dispose d'un outil, Vault, conçu spécifiquement pour gérer ce type de secrets.

2.2 Chiffrement avec Ansible Vault

2.2.1 Créer un fichier chiffré

Dans un premier temps, nous allons simplement remplacer notre fichier users.yml par un fichier entièrement chiffré, à l'aide de Ansible Vault, nommé secrets.yml. Commençons par créer le fichier à l'aide de la commande ansible-vault :

```
$ ansible-vault create
secrets.yml
New Vault password:
Confirm New Vault password:
```

Sans surprise, à la création du fichier chiffré, on nous demande de fournir un mot de passe. Une fois celui-ci fourni, la commande va lancer l'éditeur de texte par défaut du système.

Dans beaucoup de distributions, cet éditeur de texte est 'vi'. Si vous n'êtes pas habitué à utiliser cet éditeur, n'oubliez pas d'indiquer à Ansible Vault d'utiliser un autre éditeur à l'aide de la variable d'environnement EDITOR. La plupart des distributions disposent de l'éditeur nano, beaucoup plus simple à prendre en main :

```
export EDITOR=nano
```

Une fois au sein de l'éditeur, ajoutez le contenu du fichier users.yml dans le fichier secrets.yml. Quand vous quittez l'éditeur, le fichier résultant a bien été chiffré :

```
$ cat secrets.yml
$ANSIBLE_VAULT;1.1;AES256
653930636636396466643065363264333535653838336638643665316231363 5
6263623362663132
313165656430653035346338656662333266356562633964 0a30653261393634
3235336333623232
656130623839303363316233333631316635663662616166383826138373033
3365386265313064
323036663263653133 0a373961333631636662623663626436663639643137 38
6337666434323633
636361626435353435353365653134363465653337626535623730393362626 4
3165643365653138
366639396431383663376533643535383135636631663331336234383563333 4
6662666236663137
393639633537343732386239343836663238636539353935653264616332386 4
6162363831646362
643438366535396135386337303864323535313063663665393364613161346 6
3862623665303237
633839353965323433626536393131623161666265326336373437306363323 3
3964373665353333
656463323934363761656166373934376436303738613734626 6
```

Il est bien évidemment possible d'accéder à nouveau au contenu du fichier, toujours à l'aide de la commande ansible-vault :

```
$ ansible-vault edit secrets.yml
Vault password:
```

Remplaçons maintenant notre fichier users.yml par secrets.yml dans notre script Ansible :

```
...
become_method: sudo
vars_files:
  - secrets.yml
tasks:
...
```

2.2.2 Mise en place d'un fichier chiffré avec Ansible

Bien évidemment, le fichier étant désormais chiffré, Ansible est incapable d'en utiliser le contenu :

```
$ sudo ansible-playbook vsftd.yml
 [WARNING]: provided hosts list is empty,
only localhost is available. Note that the
implicit localhost does not match 'all'

ERROR! Attempting to decrypt but no vault
secrets found
```

Pour permettre à Ansible de lire ce fichier, il faut lui transmettre le mot de passe utilisé lors de la création du fichier. Pour ce faire, on peut utiliser l'option `--ask-vault-pass`, qui va déclencher, au démarrage de Ansible, la demande de saisie du mot de passe :

```
$ sudo ansible-playbook vsftd.yml --ask-
vault-pass
Vault password:
 [WARNING]: provided hosts list is empty,
only localhost is available. Note that the
implicit localhost does not match 'all'


PLAY [ftp server installed] ***************
**************************************

TASK [latest vsftpd version installed]
...
```

Néanmoins, si la saisie de mot de passe est bien adaptée à une utilisation interactive de Ansible, elle pose rapidement des problèmes si l'on souhaite automatiser les exécutions de notre script. Il est donc souvent plus pratique de placer ce mot de passe au sein d'un fichier, ce que permet Ansible à l'aide de l'option `--vault-password-file` :

```
$ sudo ansible-playbook --vault-password-
file=vault.pass
 [WARNING]: provided hosts list is empty,
only localhost is available. Note that the
implicit localhost does not match 'all'
PLAY [ftp server installed] ***************
**************************************

TASK [latest vsftpd version installed] ****
**************************************
ok: [localhost]
...
```

2.2.3 Changer le mot de passe d'un fichier chiffré

Il est bien évidemment possible de changer le mot de passe associé à un fichier chiffré. Là encore, Ansible Vault fournit un outil pour faciliter autant que possible le travail :

```
$ ansible-vault rekey secret.yml
Vault password: redhat
New Vault password: RedHat
Confirm New Vault password: RedHat
Rekey successful
```

2.2.4 Chiffrer et déchiffrer un fichier existant

Pour commencer à prendre en main Ansible Vault, nous avons opté pour la création d'un nouveau fichier. Néanmoins, il est tout à fait possible de simplement chiffrer le fichier `users.yml` :

```
$ ansible-vault encrypt users.yml
New Vault password:
Confirm New Vault password:
Encryption successful
$ cat users.yml
$ANSIBLE_VAULT;1.1;AES256
613763633138376662333061633166376632336437626430343636343930623965366537396362636165393238306563656561336230323433303566666663330a623561353230663261623435373831
```

```
62393666623662643935396635333863653836336132613232539343466646561333931373531383365386332303430383138306a6337383636303038326638636336666323032353537376634623634636533326536393438373936393539366134313834373333663062666563666635353831663637356430626665363666353538316637356430626665363666353538316637356430626665363666353538316
```

Il nous suffit maintenant de placer l'appel à la fonction password_hash au sein de notre script et le tour est joué :

```
    - name: "Create user accounts for the
FTP server"
      user:
        name: "{{ item.username }}"
        password: "{{ item.password |
password_hash('sha512') }}"
      with_items: "{{ ftp_users }}"
```

4. RÉCAPITULATIF

Une fois tous les éléments décrits ci-dessus mis en place, notre script complet est donc :

```
---
- name: ftp server installed
  hosts: localhost
  gather_facts: no
  become: yes
  become_method: sudo
  vars_files:
    - secrets.yml
  tasks:
    - name: latest vsftpd version
installed
      yum:
        name: vsftpd
        state: latest

    - name: latest firewalld version is
installed
      yum:
        name: firewalld
        state: latest

    - name: vsftpd is enabled and running
      service:
        name: vsftpd
        enabled: true
        state: started

    - name: firewalld is enabled and
running
      service:
        name: firewalld
        enabled: true
        state: started

    - name: allow ftp service
      firewalld:
        service: ftp
        permanent: true
        state: enabled
        immediate: yes

    - name: "Create user accounts for the
FTP server"
      user:
        name: "{{ item.username }}"
        password: "{{ item.password |
password_hash('sha512') }}"
      with_items: "{{ ftp_users }}"
```

Et désormais, son exécution se déroule sans erreur ni alerte :

```
$ sudo ansible-playbook --vault-password-
file=vault.pass vsftd.yml
 [WARNING]: provided hosts list is empty,
only localhost is available. Note that the
implicit localhost does not match 'all'

PLAY [ftp server installed] ***************
*******************************************
*******************************************
*******************************************
**************************

TASK [latest vsftpd version installed] ****
*******************************************
*******************************************
*******************************************
**************************
ok: [localhost]

TASK [latest firewalld version is
installed] ********************************
*******************************************
*******************************************
*******************************************
************************************
ok: [localhost]

TASK [vsftpd is enabled and running] *****
*******************************************
*******************************************
*******************************************
*******************************
ok: [localhost]

TASK [firewalld is enabled and running] ***
*******************************************
```

```
**********************************************
**********************************************
****************************
ok: [localhost]

TASK [allow ftp service] ******************
**********************************************
**********************************************
**********************************************
**********************************************
****************************
ok: [localhost]

TASK [Create user accounts for the FTP
server] ***********************************
**********************************************
**********************************************
*********************************

changed: [localhost] => (item={'username':
'mike', 'password': 'mike-mot-de-passe'})
changed: [localhost] => (item={'username':
'bob', 'password': 'bob-mot-de-passe'})

PLAY RECAP *********************************
**********************************************
**********************************************
**********************************************
****************************
localhost                  : ok=6
changed=1    unreachable=0    failed=0
```

CONCLUSION

La gestion des secrets est certainement l'un des aspects les plus difficiles des métiers de l'informatique. Il faut s'assurer que, à chaque étape, le secret requis est présent, mais aussi, que ce dernier reste toujours le plus confidentiel possible. Cette problématique est donc au cœur du métier de Ansible, mais fort heureusement, comme l'aura, nous l'espérons, illustré cet article, on dispose tous les outils nécessaires — qu'il s'agisse de chiffrer un fichier utilisé par Ansible qui contient des données sensibles, ou simplement de mettre en place le hachage cryptographique. ■

RÉFÉRENCE

[1] https://connect.ed-diamond.com/Linux-Pratique/LP-113/L-automatisation-dans-vos-systemes-d-informations-avec-Ansible

TOUJOURS DISPONIBLE !

LINUX PRATIQUE n°113

N°113
COMPRENDRE, UTILISER & ADMINISTRER LINUX
GNU LINUX PRATIQUE
MAI JUIN 2019
ÉDUCATION
Apprenez à créer un jeu de réflexion avec Pygame Zero p. 80
CODE
Intégrez une gestion des ACL à vos applications PHP p. 67
ENTREPRISE
Comment organiser votre communication sur Mastodon ? p. 90
SYSTÈME
Installez automatiquement Debian sans support d'installation p. 22
SYSTÈME
SIMPLIFIEZ L'ADMINISTRATION DE VOS MACHINES AVEC ANSIBLE ! p. 30
• Pourquoi automatiser ?
• Configurer Ansible
• Cas pratique d'automatisation
TUTORIELS
BUREAUTIQUE
Recadrez, annotez, compressez, protégez, éditez et gérez vos fichiers PDF p. 08
PHOTOS
Optimisez vos photographies avec GIMP avant leur publication sur Internet p. 16
AUTO-HÉBERGEMENT
Centralisez la gestion des vos applications auto-hébergées avec Sandstorm p. 58
SÉCURITÉ
Isolez vos processus grâce à AppArmor p. 50

SIMPLIFIEZ L'ADMINISTRATION DE VOS MACHINES AVEC ANSIBLE !

SUR :

https://www.ed-diamond.com

Authentification de l'accès à votre réseau : MISE EN PLACE D'UN PORTAIL CAPTIF ET D'UN SERVICE 802.1X

NICOLAS GRENECHE

UN PORTAIL CAPTIF EST UN ÉLÉMENT DE CONTRÔLE MANDATAIRE RÉGULANT L'ACCÈS AU RÉSEAU POUR LES CLIENTS ÉQUIPÉS D'UN NAVIGATEUR WEB. DANS CET ARTICLE, NOUS ALLONS VOIR COMMENT INTÉGRER CET ÉLÉMENT DANS UNE INFRASTRUCTURE POUR AUTHENTIFIER LES CLIENTS CONNECTÉS EN WI-FI AVANT LEUR ACCÈS EFFECTIF AU RÉSEAU EXTÉRIEUR. NOUS ALLONS ÉGALEMENT PRÉSENTER LE 802.1X QUI VISE À AUTHENTIFIER LES UTILISATEURS AVANT TOUT ACCÈS AU RÉSEAU.

Les solutions de portails captifs fonctionnent toutes sur le même principe :

1) L'utilisateur tente d'aller sur Internet ;
2) Il est redirigé sur une page d'authentification ;
3) Il entre son identifiant et son mot de passe ;
4) Un ensemble de règles de filtrage est joué sur le portail captif pour règlementer son accès au réseau externe ;
5) Il sort sur le réseau conformément aux règles générées.

Dans cet article, nous allons aborder la mise en place d'un tel portail à l'aide de la solution pfSense sur une machine dédiée. Nous allons également présenter une solution alternative d'authentification des utilisateurs avant leur accès au réseau sous la forme d'un service 802.1X embarqué directement sur la borne Wi-fi grâce à OpenWRT.

1. PFSENSE

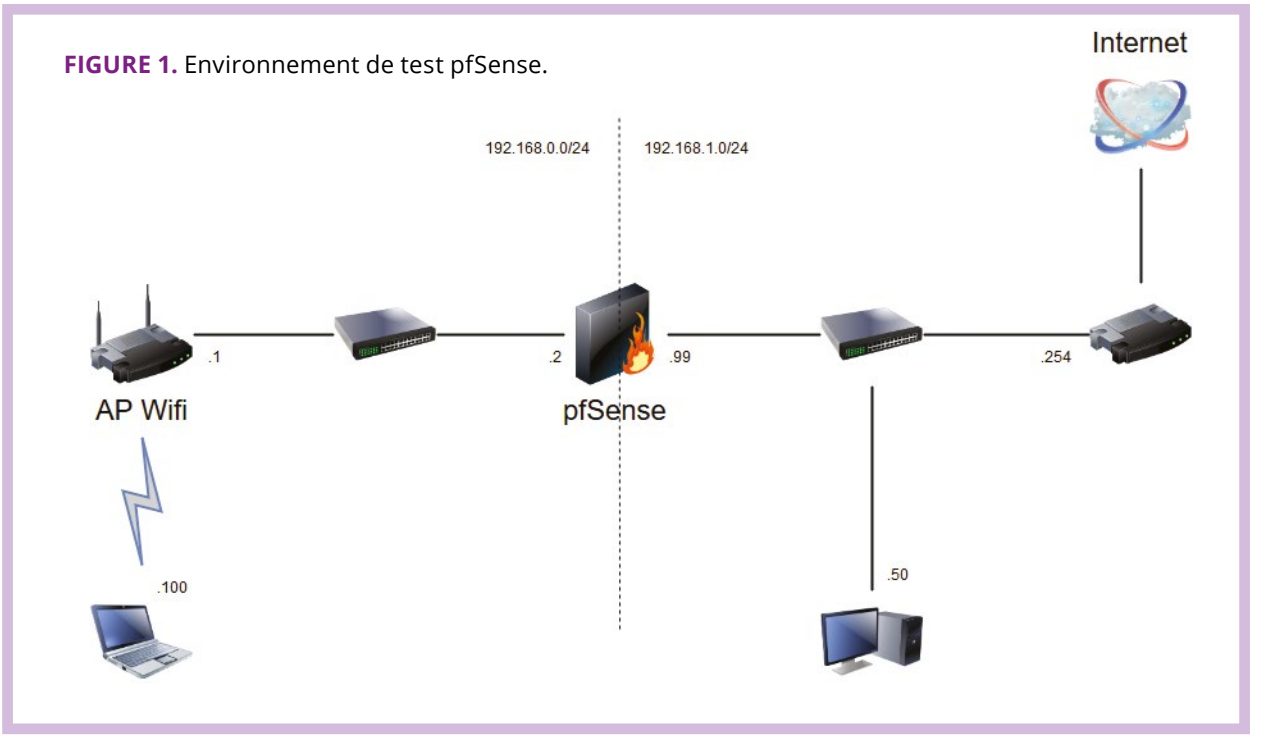
Le logiciel pfSense est une solution d'UTM (*Unified Threat Management*) libre. Un UTM est un boîtier regroupant de multiples fonctionnalités de sécurité comme le filtrage réseau, la détection/prévention d'intrusions, un service de VPN, proxy web ou encore un portail captif. C'est sur cette dernière fonctionnalité que nous allons nous attarder. Commençons par présenter l'environnement de test.

1.1 Environnement de test

Pour faire nos tests, dédions une machine physique à pfSense. Cette machine dispose de deux interfaces réseaux. La première est reliée à un commutateur sur lequel la borne Wi-fi est raccordée (partie gauche de la figure 1) tandis que la seconde est connectée au réseau extérieur (qui a accès à Internet). La première notion à clarifier pour l'installation et l'exploitation de pfSense est celle de LAN/WAN.

Un LAN (*Local Area Network*) est stricto sensu un domaine de broadcast Ethernet. En pratique, cela concerne les machines connectées au même équipement de commutation (switch physique, borne Wi-fi etc.). Ces équipements

FIGURE 1. Environnement de test pfSense.



de commutations peuvent être empilés (c'est-à-dire raccordés les uns aux autres) pour accroître le nombre de ports disponibles sur le LAN (ou, comme dans notre exemple, ouvrir un réseau filaire au sans fil).

Le WAN (*Wide Area Network*) est un réseau dit étendu. L'idée est que le WAN connecte un ou plusieurs LAN à Internet. Attention, cette définition est extrêmement grossière, car le WAN peut être un backbone de routeurs connectant une multinationale au restant du monde ou une simple interface estampillée « WAN » sur un routeur (ou une box) connectée au réseau téléphonique (ou fibre). Ces deux définitions sont sujettes à interprétation, car fortement dépendantes du contexte.

Pour nous, le LAN est le réseau 192.168.0.0/24 avec la borne occupant l'adresse 192.168.0.1 et la patte LAN du pfSense en 192.168.0.2. Le service DHCP est activé sur cette patte. Le réseau extérieur est en 192.168.1.0/24. On y retrouve la patte WAN du pfSense en 192.168.1.99 et le routeur connecté à Internet en 192.168.1.254. Ce routeur étant une box internet, il fait aussi office de serveur DNS.

1.2 Configuration de la borne

Commençons par configurer la borne. Il est intéressant de constater qu'elle dispose elle-même d'une interface estampillée WAN et d'une autre LAN.

Ça raccroche avec ce que je mentionnais plus haut à savoir que ces deux notions sont assez floues (relevant quasiment de la tradition orale). En effet, le WAN et une simple interface réseau RJ45 et le LAN un bridge de quatre interfaces physiques RJ45 et des deux interfaces Wi-fi pour constituer un petit commutateur Ethernet embarqué directement sur la borne unifiant les connexions filaires et sans fils. Le point d'accès (AP) Wi-fi utilisé est un TP-LINK Archer C7. La caractéristique intéressante est qu'il embarque un logiciel d'exploitation grandement basé sur la distribution Linux libre OpenWRT dédiée aux points d'accès Wi-fi, nous y reviendrons par la suite.

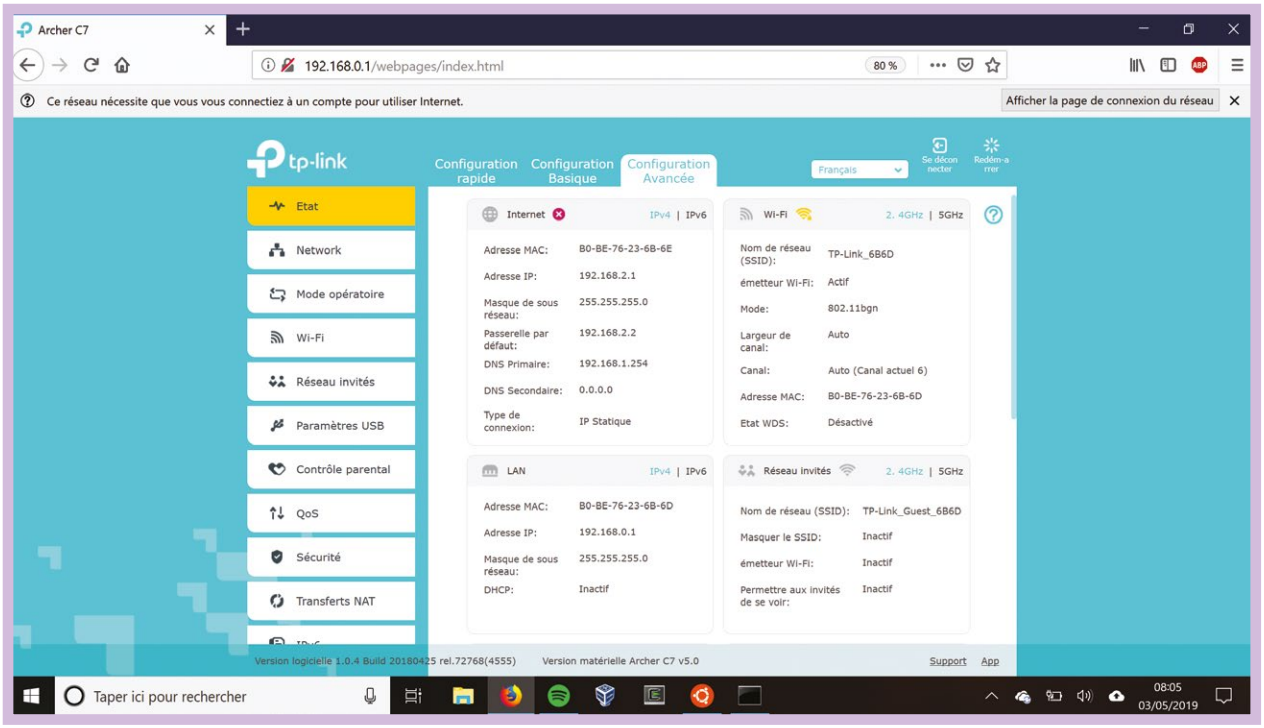


FIGURE 2. Configuration de la borne.

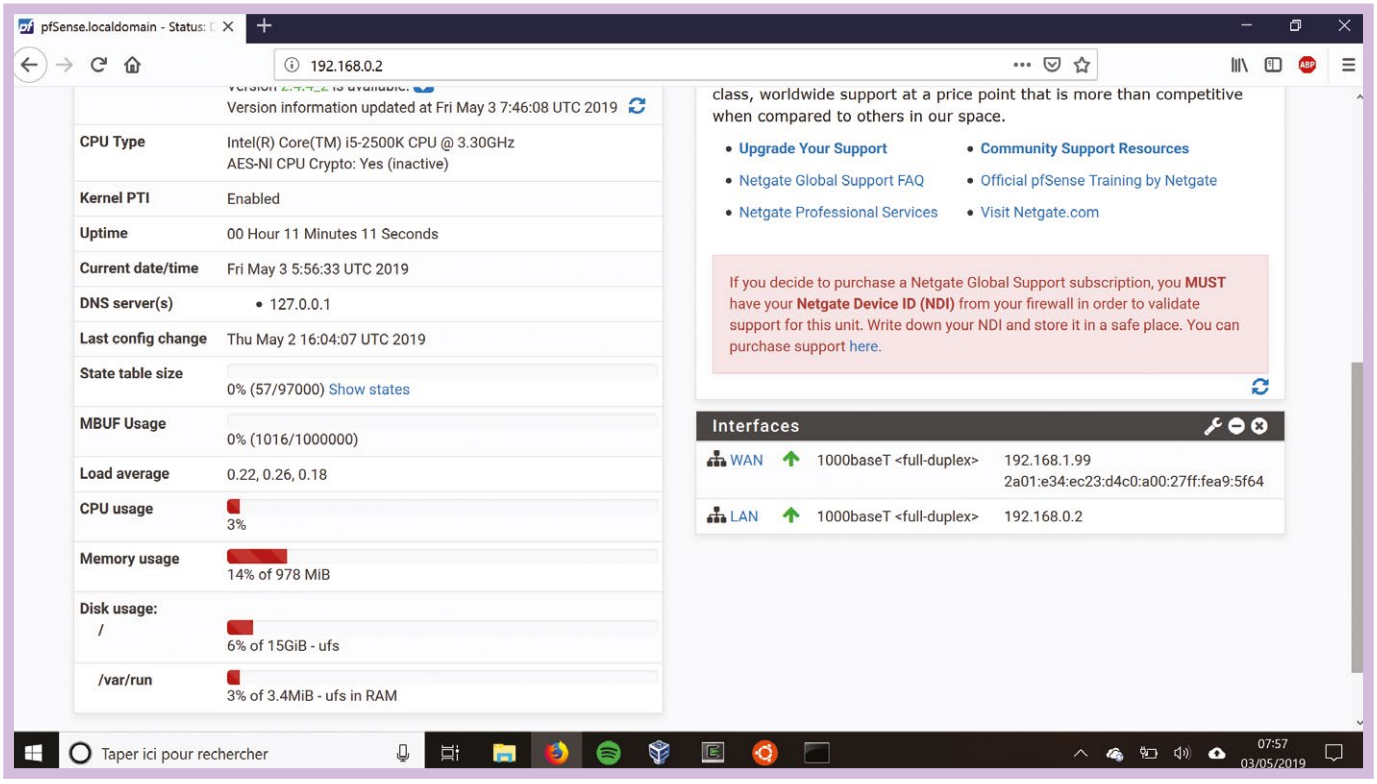


FIGURE 3. Page d'accueil de pfSense.

Dans notre exemple, seule l'interface LAN de la borne est configurée. Cette interface est connectée à notre commutateur sur lequel la patte LAN du pfSense est également présente. En effet, le concept de portail captif ne se limite pas aux réseaux sans fil. Il y a deux étapes nécessaires au bon fonctionnement de la borne :

1) donner une adresse à l'interface LAN pour gérer la borne via l'interface web (ou en SSH), ici il s'agit de la 192.168.0.1 ;
2) déclarer un SSID (*Service Set IDentifier*).

Le SSID est le nom du réseau sans fil qui est affiché par les systèmes des utilisateurs en recherche de connexion. Optionnellement, il est possible d'ajouter une clé pour s'attacher au réseau Wi-fi (option conseillée tant que notre pfSense n'est pas opérationnel). On notera dans la capture de la figure 2 qu'une interface WAN est configurée, mais l'adresse est bidon, l'interface n'est même pas branchée (elle est marquée d'une croix).

1.3 Configuration de pfSense

L'installation de pfSense est extrêmement bien décrite dans cette documentation **[1]**. Le seul point méritant une explication est la notion de VLAN **[2]**. Nous n'allons pas les utiliser, mais ils sont pris en charge par pfSense. Un VLAN est un moyen de segmenter les domaines de broadcast sur un équipement physique de commutation en vue de les faire cohabiter avec une certaine étanchéité. Une fois ces étapes accomplies, il faut configurer les interfaces LAN et WAN. C'est exactement le même principe que pour la borne Wi-fi.

L'interface LAN est la passerelle par défaut des machines situées soit sur le réseau filaire du commutateur, soit sur le réseau sans fil. Au lancement de pfSense, il faut vérifier que l'interface physique raccordée au réseau accueillant les clients sans fil est bien positionnée en LAN et que celle connectée au monde extérieur est en WAN. Si ce n'est pas le cas, il faut choisir l'option numéro 1 : ***Assign Interfaces***. Le programme de

configuration va ensuite vous demander d'entrer le nom des interfaces à assigner au WAN puis au LAN. Ensuite, il faut leur affecter des adresses IP en choisissent l'option numéro 2 : ***Set Interface(s) IP address***. On choisit l'interface à configurer. Commençons par le LAN. Nous lui affectons l'IP 192.168.0.2. Pour le masque (*bit count*), nous choisissons 24. Et nous n'entrons pas de passerelle par défaut. On ne configure pas non plus l'IPv6. Il faut ensuite activer le DHCP sur l'interface. La dernière question n'est pas très explicite : « Do you want to revert to HTTP as the webConfigurator protocol ? ». Par défaut, pfSense configure un accès HTTPS à l'interface d'administration. Nous allons rester en HTTP pour ne pas alourdir cet article avec la gestion des certificats. Nous allons donc répondre oui. À l'issue de ces manipulations, l'interface d'administration est accessible sur **http://192.168.0.1**.

Il reste l'interface WAN à configurer. On retourne sur l'option numéro 2 utilisée précédemment et cette fois-ci il faut choisir l'interface WAN. La première question est de savoir si on veut configurer l'interface en client d'un serveur DHCP. La réponse est non, nous allons opter pour une configuration statique. Nous entrons ensuite l'IP de l'interface 192.168.1.99 et 24 pour le masque de sous-réseau. Cette fois-ci, nous allons fixer une adresse de passerelle qui est celle du routeur connecté à Internet : 192.168.1.254. Enfin, comme précédemment, nous n'activons rien de relatif à IPv6. Nous pouvons maintenant nous connecter sur l'interface d'administration avec le compte par défaut « admin » et le mot de passe « pfsense » et nous arrivons sur l'écran d'accueil de pfSense (figure 3, page précédente).

Une fois connecté à l'interface d'administration, il faut fixer quelques paramètres sur le service DHCP. Dans la section ***Services***, il faut aller sur ***DHCP Server***. Les paramètres qui vont nous intéresser sont ***Subnet***, ***Subnet mask*** et ***Range***. Ces trois paramètres devraient être initialisés à des valeurs correctes pour nos manipulations, mais dans le doute, ***Subnet*** est à 192.168.0.0, ***Subnet mask*** à 24 et ***Range*** de 100 à 199. Les deux derniers paramètres à gérer sont ***DNS servers*** et ***Gateway***, soit le serveur DNS à servir aux clients et la passerelle par défaut. Pour le segment LAN, la passerelle est l'interface de la machine pfSense donc 192.168.0.2 et le serveur DNS est le cache hébergé sur le routeur de sortie, donc 192.168.1.254. Avec ces paramètres, les clients connectés à la borne devraient pouvoir sortir sur le réseau externe.

1.4 Configuration du portail captif

Avant d'entrer dans le vif de la configuration du portail, il convient de suivre le périple des paquets émis par une machine domiciliée sur le réseau sans fil derrière le pfSense. Lorsque la machine émet le paquet, si son adresse de destination n'est pas sur le réseau LAN, alors le paquet est envoyé à la passerelle par défaut. Cette passerelle est l'interface LAN du pfSense. Une fois le paquet arrivé sur la passerelle, il est confronté aux règles de filtrage définies sur l'interface LAN. Si le paquet est autorisé, alors le noyau transfère le paquet de l'interface LAN au WAN, car le passage de paquet d'une interface à l'autre est autorisé par la variable du noyau `net.inet.ip.forwarding` positionnée à 1. À ce niveau-là, l'adresse source du paquet est natée avec celle de l'interface WAN. En conséquence, vus du réseau externe (WAN) tous les paquets issus du réseau sans fil arrivent avec la même IP source, ce qui peut être un souci majeur dans le processus de monitoring réseau. Il peut donc être nécessaire d'instrumenter la passerelle pfSense dans un contexte professionnel **[3]**. Une fois naté, le paquet est envoyé vers la passerelle par défaut de la machine pfSense qui n'est autre que le routeur de sortie du réseau WAN donc Internet. Enfin, le paquet sort.

Le portail captif intercepte donc le trafic avant qu'il ne sorte de l'interface. La première décision à prendre est de savoir où placer ce portail. Nous allons le mettre au plus près des clients sans fil, c'est-à-dire sur l'interface LAN du pfSense. Pour accéder à la configuration du portail, il faut sélectionner l'option ***Captive Portal*** du menu ***Services***. Ensuite, on clique sur ***Add*** pour ajouter une instance de portail. Pour pfSense, un portail sert une zone, il faut donc la nommer. Nous l'appellerons Wifi. Il faut cliquer sur ***Save & Continue*** pour enregistrer l'instance de portail dans la configuration de pfSense. Un écran demandant d'activer le portail arrive, il faut cocher l'option et cliquer sur ***Save***. Enfin, la configuration du portail s'affiche. Ici, on ne va fixer que deux paramètres pour avoir une instance minimale fonctionnelle :

1) l'interface sur laquelle le portail va s'attacher ;
2) la localisation de la base des comptes autorisés à utiliser le portail.

Pour attacher le portail à l'interface, il faut choir ***LAN*** pour l'attribut ***Interfaces*** (figure 4).

Toujours dans le souci de créer un portail minimal, nous allons adosser les utilisateurs du portail à une

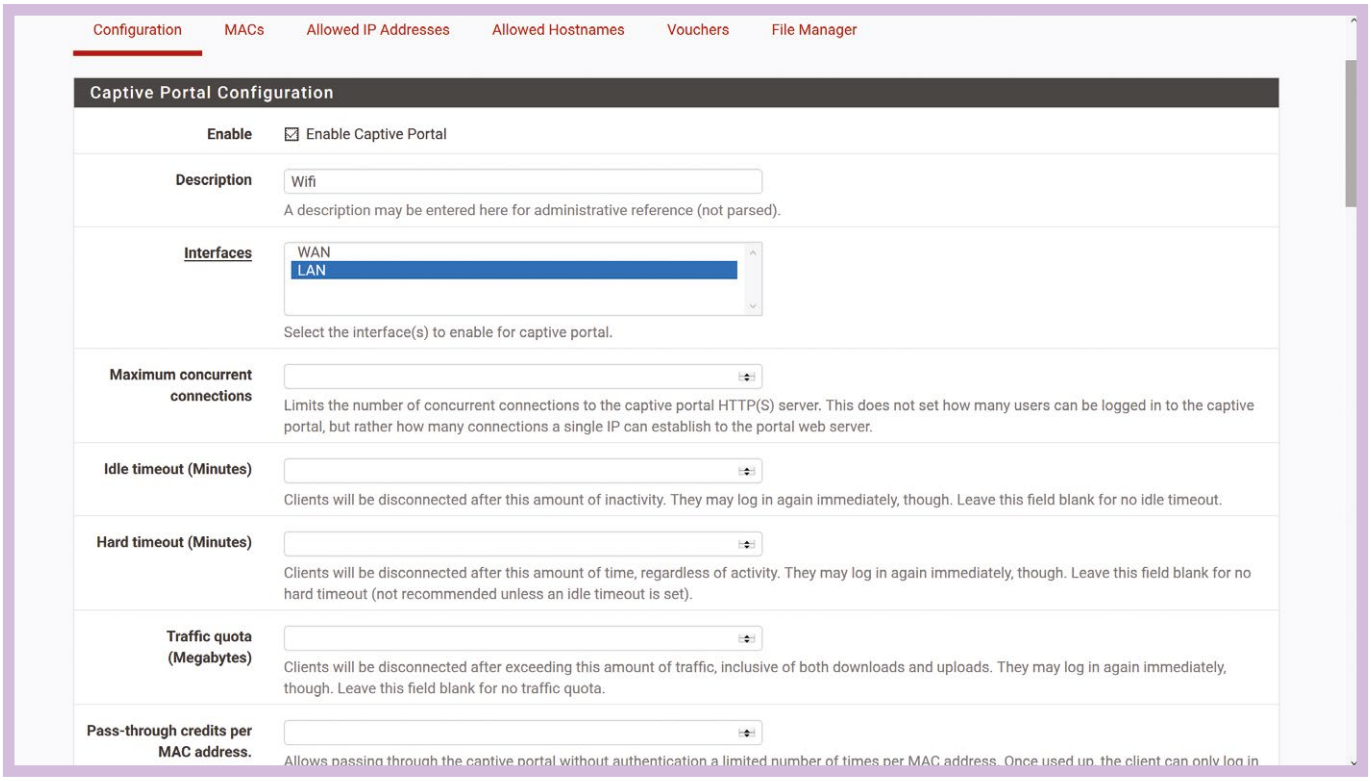

Configuration
MACs
Allowed IP Addresses
Allowed Hostnames
Vouchers
File Manager
Captive Portal Configuration
Enable
Enable Captive Portal
Description
Wifi
A description may be entered here for administrative reference (not parsed).
Interfaces
WAN
LAN
Select the interface(s) to enable for captive portal.
Maximum concurrent connections
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout (Minutes)
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Traffic quota (Megabytes)
Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.
Pass-through credits per MAC address.
Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in

FIGURE 4. Attacher le portail à l'interface LAN.

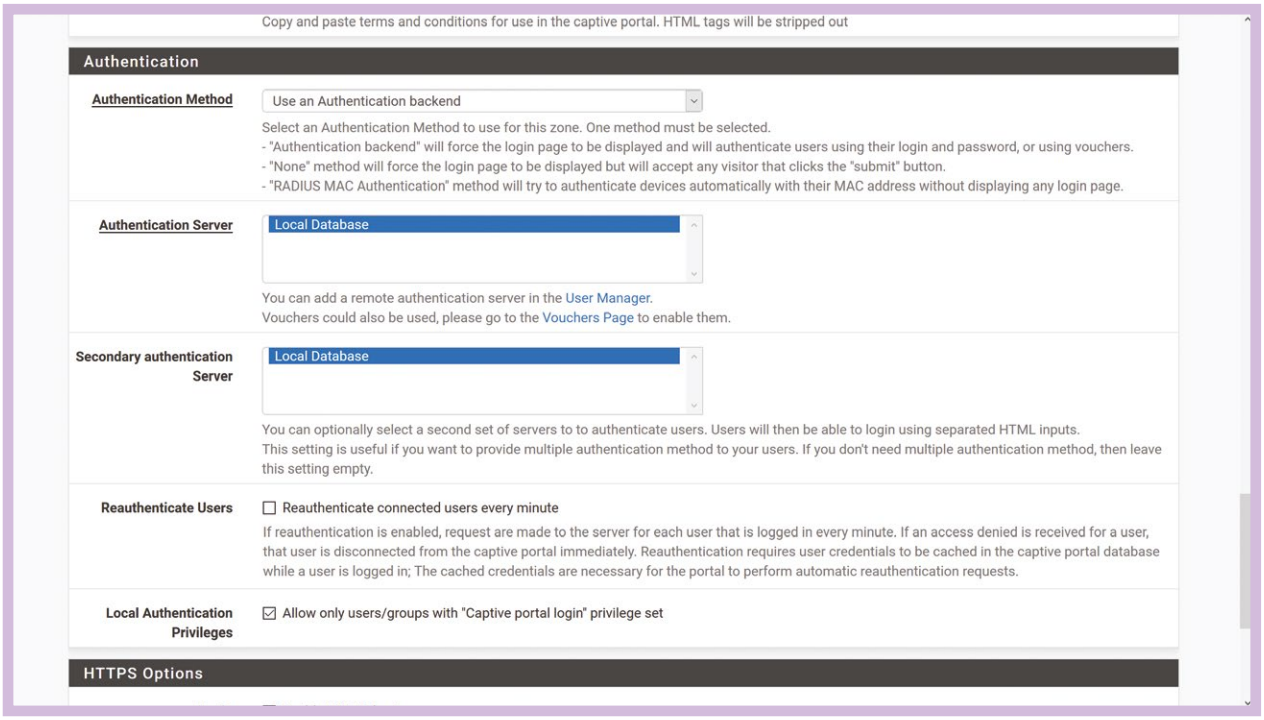

Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out
Authentication
Authentication Method
Use an Authentication backend
Select an Authentication Method to use for this zone. One method must be selected.
- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
Authentication Server
Local Database
You can add a remote authentication server in the User Manager.
Vouchers could also be used, please go to the Vouchers Page to enable them.
Secondary authentication Server
Local Database
You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs.
This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.
Reauthenticate Users
Reauthenticate connected users every minute
If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.
Local Authentication Privileges
Allow only users/groups with "Captive portal login" privilege set
HTTPS Options

FIGURE 5. Adosser une base de compte locale.

base locale créée sur le pfSense. Pour cela, il faut sélectionner l'option ***Use an Authentication backend*** pour l'attribut ***Authentication Method*** de la section ***Authentication***.

La dernière étape est de mettre le serveur DNS en liste blanche. En effet, pour qu'un navigateur émette une requête HTTP à intercepter par le portail, il est nécessaire qu'il puisse faire une résolution DNS au préalable pour localiser la machine à qui adresser cette requête. Cela se passe dans la section ***Allowed***

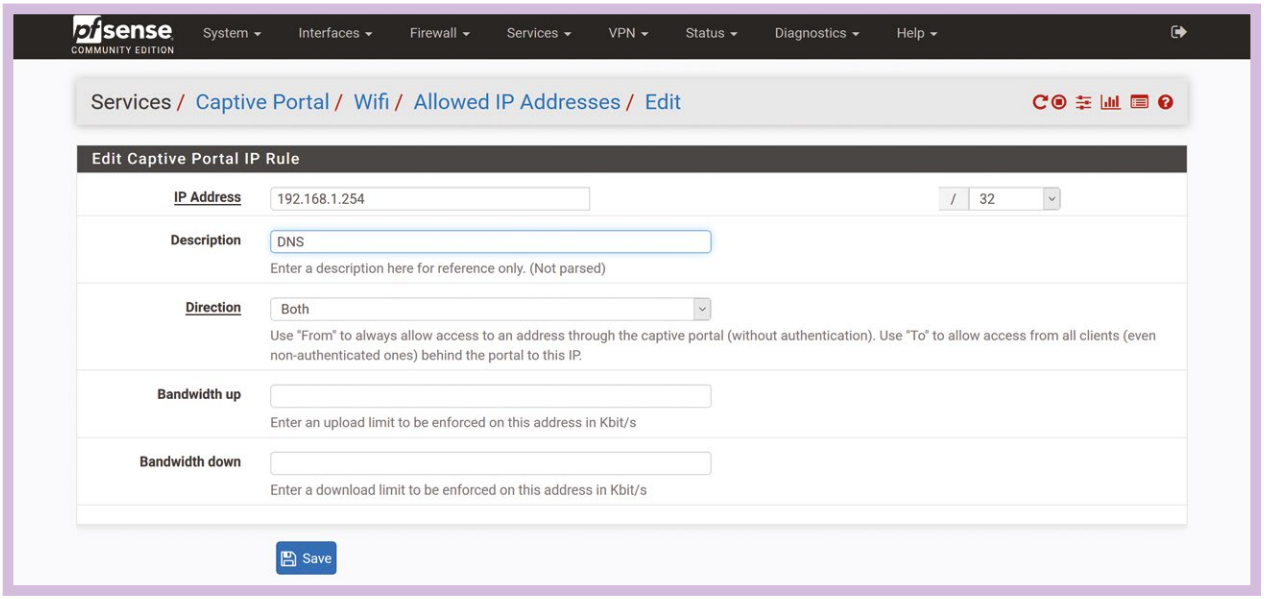

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / Captive Portal / Wifi / Allowed IP Addresses / Edit
Edit Captive Portal IP Rule
IP Address
192.168.1.254
/ 32
Description
DNS
Enter a description here for reference only. (Not parsed)
Direction
Both
Use "From" to always allow access to an address through the captive portal (without authentication). Use "To" to allow access from all clients (even non-authenticated ones) behind the portal to this IP.
Bandwidth up
Enter an upload limit to be enforced on this address in Kbit/s
Bandwidth down
Enter a download limit to be enforced on this address in Kbit/s
Save

FIGURE 6. Autorisation du serveur DNS.

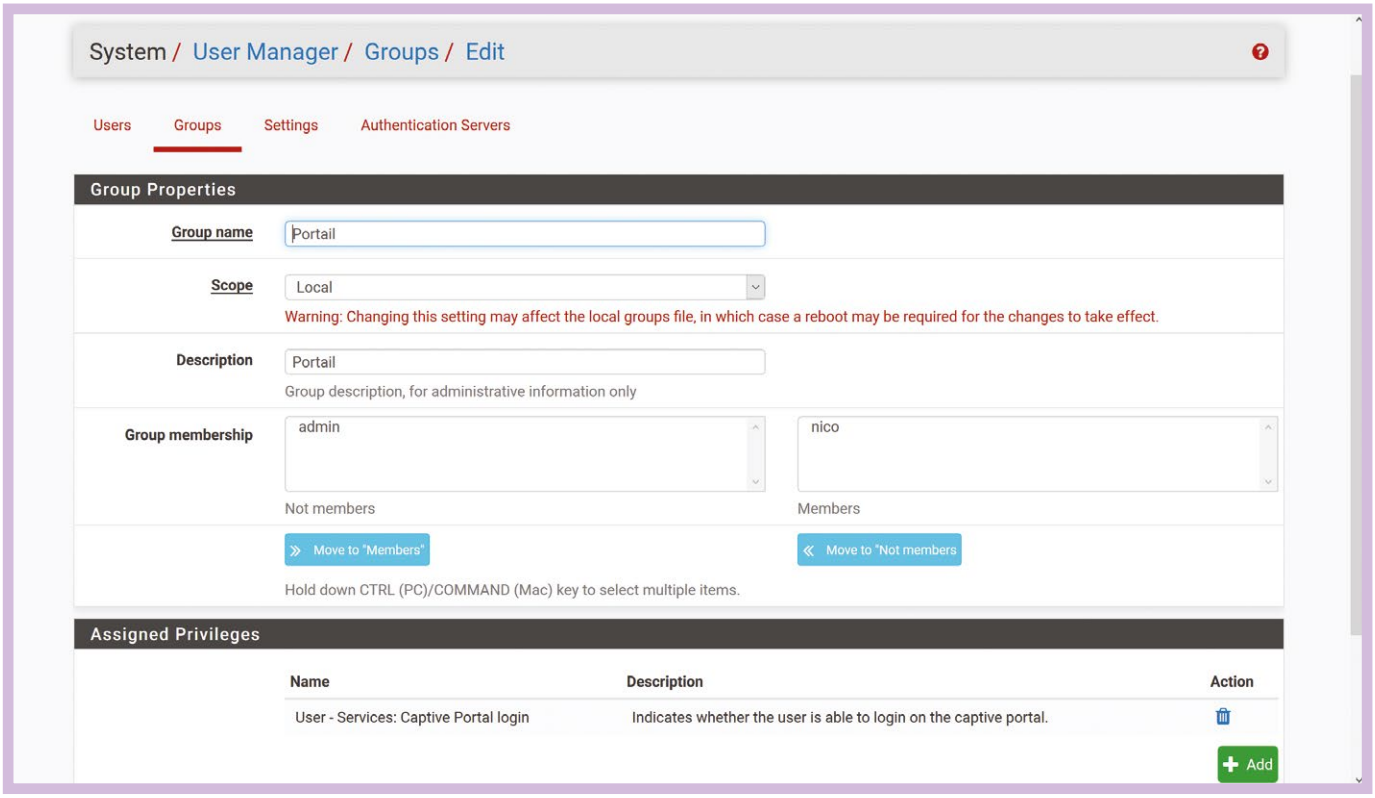


FIGURE 7. Création du groupe d'utilisateurs du portail.

IP Addresses de la configuration du portail. On doit entrer l'adresse du serveur DNS pour l'attribut ***IP Address***, soit 192.168.1.254 et le sens de communication pour l'attribut ***Direction***, soit ***Both*** (figure 6). Le portail est maintenant configuré et fonctionnel. Il ne reste plus qu'a créer les utilisateurs.

Si vous êtes dans un environnement assez chargé, il vous faudrait également considérer les deux attributs suivants dans la configuration du portail : ***Idle timeout*** et ***Hard timeout***. Le premier donne un délai en minutes au-delà duquel un utilisateur inactif est déconnecté. Le second donne un délai de déconnexion indépendamment de toute activité.

1.5 Création des utilisateurs

Nous allons ajouter des utilisateurs pour le portail. L'idée est de créer un groupe avec tous les utilisateurs autorisés à utiliser le portail. Commençons par créer le groupe. Cela se passe dans ***System*** puis ***User Manager*** puis ***Groups***. Nous créons un groupe nommé *Portail* (***Group Name***), dans le ***Scope*** *Local* (c'est-à-dire local à notre pfSense). La partie la plus importante est la section ***Assigned Privileges*** où il faut cliquer sur ***Add*** et rechercher le privilège « User – Services : Captive Portal Login » (figure 7).

Puis créons un utilisateur nommé nico. Cela se passe dans ***System*** puis ***User Manager*** puis ***Users***. Les deux paramètres importants sont le ***Username*** (identifiant) et ***Password*** (mot de passe). Dès cet écran, il est possible de positionner l'utilisateur directement dans le groupe portail (figure 8, page suivante).

Lorsque l'utilisateur va essayer d'accéder à un site web, il va tomber sur une page lui demandant de s'authentifier avant d'accéder au réseau (figure 9, page suivante). Une fois votre identifiant et votre mot de passe entrés, vous pouvez sortir sur Internet. Vos traces sont désormais authentifiées par le portail.

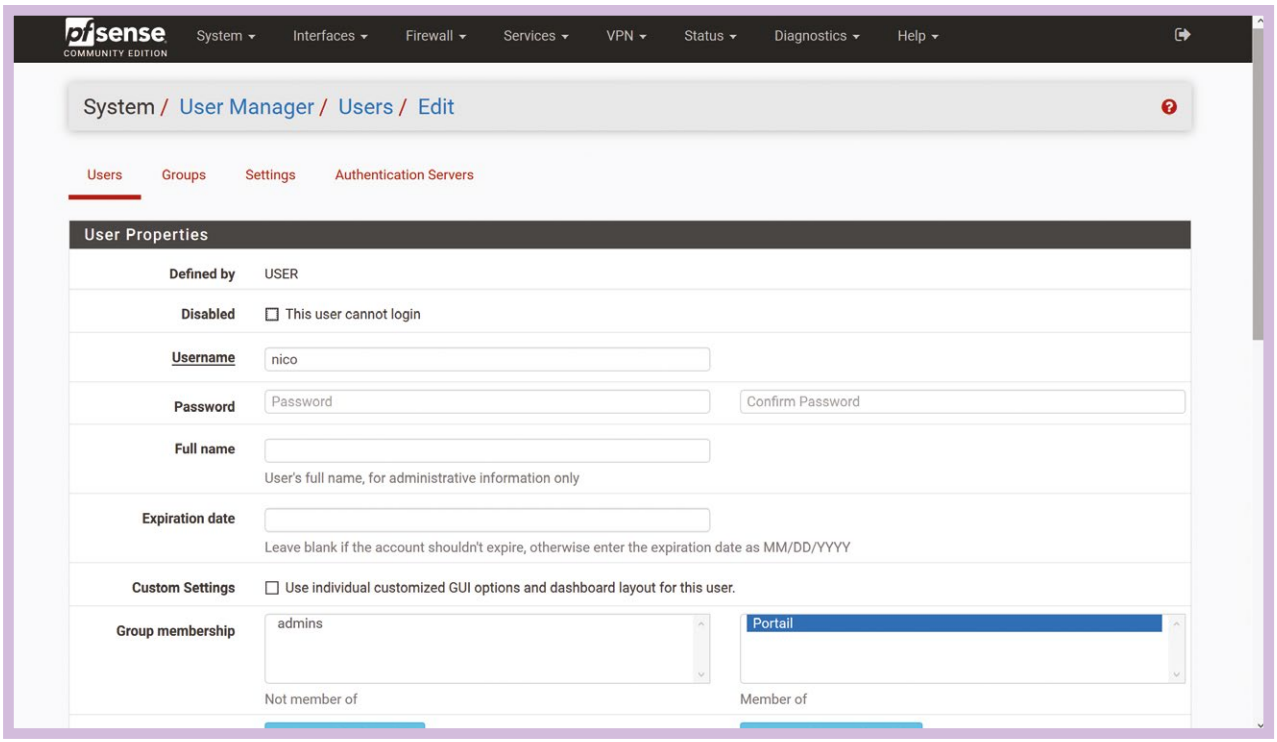


FIGURE 8. Création d'un utilisateur.

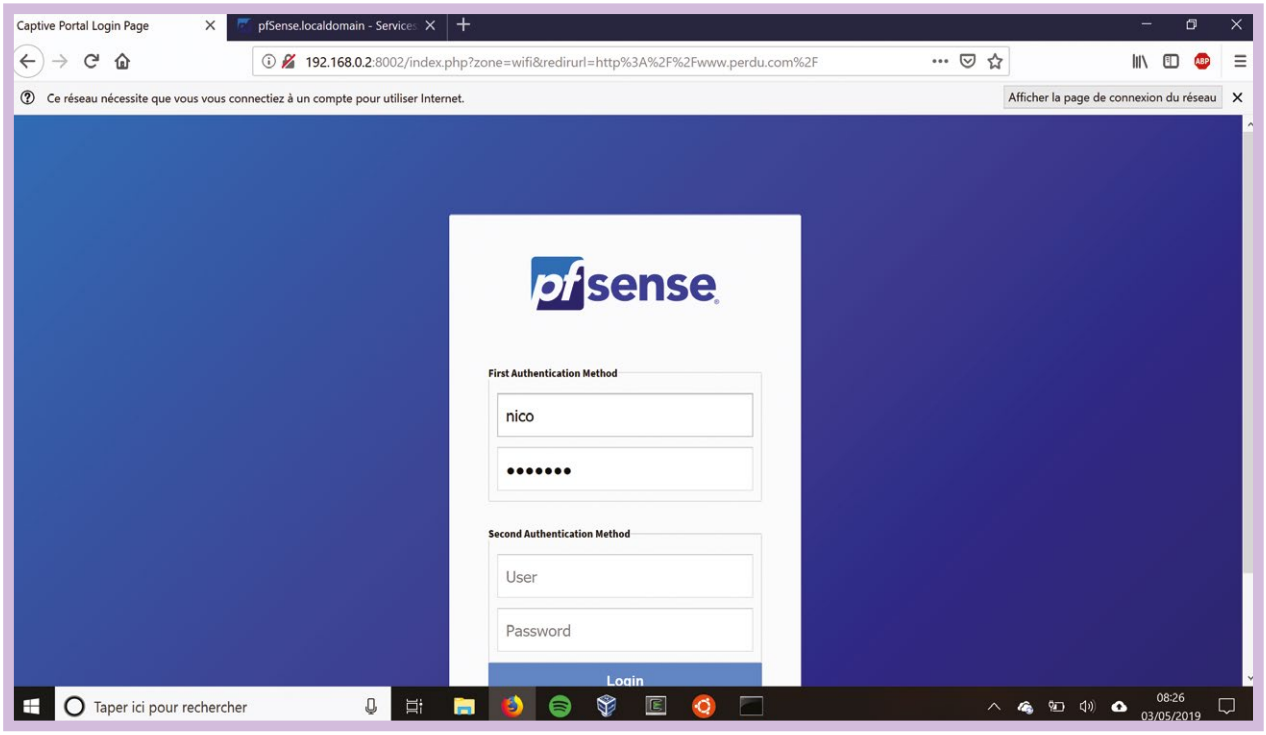


FIGURE 9. Page d'authentification du portail.

1.6 Résolution des problèmes

Si toutefois vous ne tombez pas sur la page directement il peut y avoir plusieurs raisons. La première est que vous n'avez peut-être pas autorisé les requêtes DNS. Pour vérifier, vous pouvez ouvrir un terminal et taper la commande suivante :

```
ngreneche@DESKTOP-RE130IB:~$ host www.google.fr 192.168.1.254
www.google.fr has address 216.58.204.99
www.google.fr has IPv6 address 2a00:1450:4007:80a::2003
```

Où nous demandons explicitement au serveur 192.168.1.254 de résoudre **www.google.fr**. Si cela fonctionne, peut-être qu'une notification est apparue sur votre navigateur type « Ce réseau nécessite que vous vous connectiez à un compte pour utiliser Internet ». Dans ce cas, il faut penser à la valider et vous allez arriver sur le portail. Si les problèmes persistent, vous pouvez aller voir ce qui s'affiche dans les logs du portail captif. Ils se trouvent dans ***Status > System Logs > Captive Portal Auth***. Il peut également se produire que le portail affiche une page blanche (ce n'est pas forcément lié a pfSense, ça arrive aussi avec des portails commerciaux). Dans ce cas, c'est souvent que la déconnexion de l'utilisateur s'est mal passée. Il faut procéder à une déconnexion manuelle (et/ou réduire le ***Idle Timeout***). Vous pouvez visualiser les utilisateurs connectés dans la section ***Status > Captive Portal > Wifi*** (c'est le nom de notre zone).

Côté client, une variable qui peut aussi influer sur le comportement du portail est l'activation ou non de la détection automatique de portail captif. Le système va essayer d'accéder à une URL qu'il connaît bien et s'il récupère la page attendue il conclut qu'il n'a pas besoin de passer par un portail pour s'authentifier. Dans le cas contraire, il ouvre la fenêtre de connexion.

2. OPENWRT

OpenWRT est une distribution Linux adaptée aux équipements type routeurs, point d'accès Wi-fi, etc. Dans notre article, nous allons remplacer le système d'exploitation du routeur par une instance d'OpenWRT pour proposer une authentification 802.X à nos utilisateurs. La différence avec la partie d'avant sur pfSense est que l'utilisateur devra entrer un identifiant et un mot de passe pour obtenir la connexion physique au réseau. En effet, dans le cas précédent, l'utilisateur avait une connexion réseau, car il devait être capable d'accéder au portail pour s'authentifier ainsi qu'au DNS.

2.1 Environnement de test

Notre nouvel environnement est composé d'un réseau sans fil en 192.168.0.0/24 et du même réseau local proposant l'accès externe en 192.168.1.0/24. La différence est que cette fois-ci

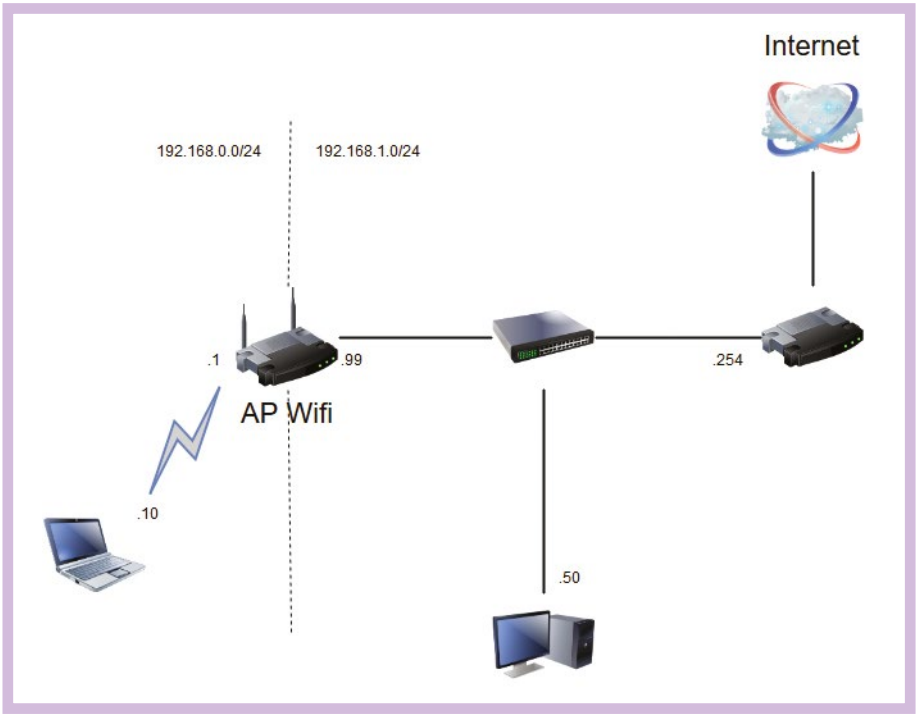


FIGURE 10. Environnement de test OpenWRT.

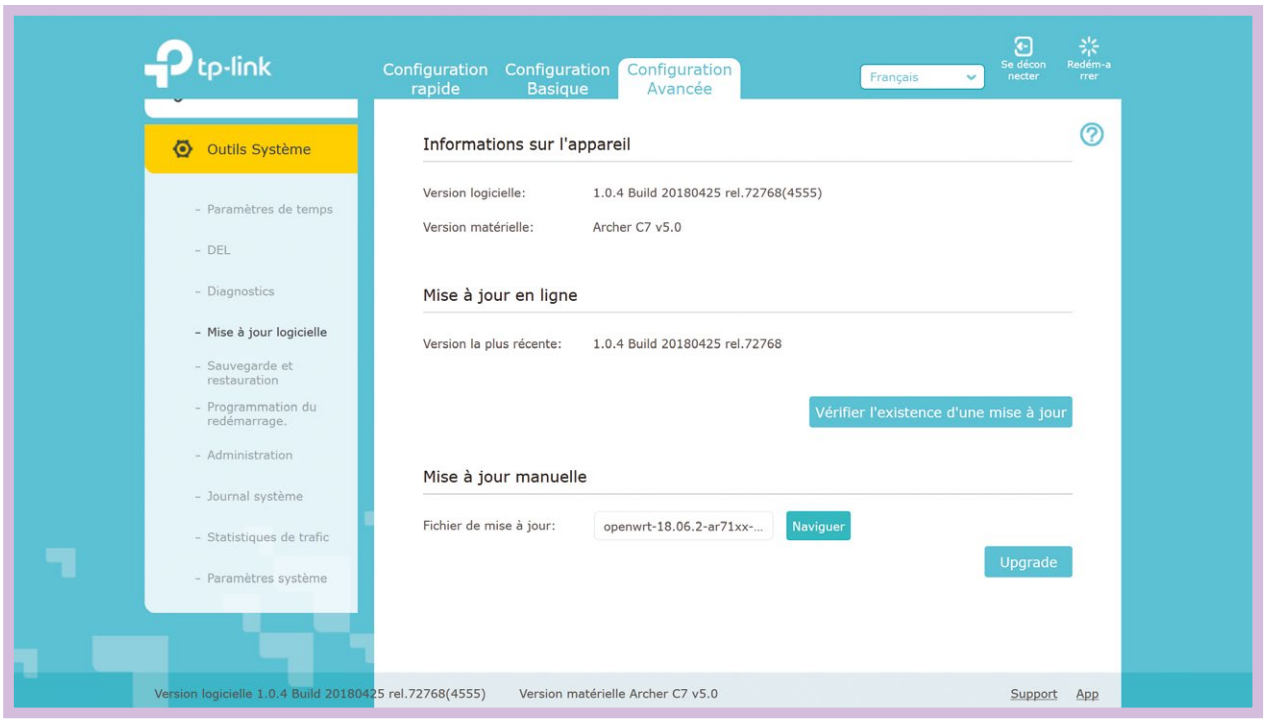


FIGURE 11. Chargement du firmware OpenWRT.

c'est la borne elle-même qui va porter les interfaces LAN et WAN. L'interface LAN en 192.168.0.1 servira le réseau sans fil tandis que l'interface WAN en 192.168.1.99 connectera notre routeur Wi-fi au monde extérieur. Le service DHCP sera embarqué directement sur la borne sur l'interface LAN pour configurer automatiquement les clients sans fil.

2.2 Configuration de la borne

Pour configurer la borne, il faut commencer par remplacer le firmware de base par celui d'OpenWRT. Avant tout, il faut contrôler la version d'OpenWRT à appliquer sur son matériel selon la matrice de compatibilité suivante **[4]**. Une fois le firmware téléchargé **[5]**, il faut le charger sur l'équipement. Pour notre borne TP-Link, cela se passe dans ***Outils Systèmes > Mise à jour logiciel***. On y trouve une rubrique ***Mise à jour manuelle*** (figure 11) dans laquelle on peut charger l'image téléchargée d'OpenWRT.

Une fois la mise à jour validée, le système est remplacé et il redémarre sous OpenWRT. On peut se brancher en filaire pour accéder à l'interface web de configuration sur **http://192.168.1.1** avec comme identifiant root, sans mot de passe. Il ne faut évidemment pas connecter l'interface WAN, car elle serait sur le même réseau que LAN ce qui poserait de gros soucis ! Une fois dans l'interface, commençons par fixer un mot de passe à root. On voit qu'une fois connecté, nous avons une bannière nous invitant à changer le mot de passe root (figure 12, page 59). En plus, nous pouvons même y activer un accès SSH. Les paramètres par défaut du service SSH sont bons (port 22, autoriser la connexion root et l'authentification par mot de passe). Pensez bien à sauvegarder et appliquer votre configuration à chaque étape.

Les deux choses à faire sont de configurer les interfaces LAN et WAN. Petite astuce, le changement de d'adresse de LAN via l'interface ne fonctionne pas forcément bien sur notre version d'OpenWRT. Nous allons donc mettre à profit le serveur SSH fraîchement installé et modifier l'adresse en ligne de commandes, cela se passe dans la section `config interface 'lan'` du fichier `/.etc/config/network` :

ABONNEZ-VOUS

N° 114
COMPRENDRE, UTILISER & ADMINISTRER LINUX
GNU LINUX PRATIQUE
JUIL. AOÛT 2019
SÉCURITÉ
Sécurisez les données sensibles de votre infrastructure avec Ansible Vault p. 38
SYSTÈME
Réaliser une sauvegarde et la restaurer avec Btrfs p. 24
SERVEUR
Installer, configurer et sécuriser un serveur Apache2 p. 30
SCIENCES
Découvrez eLabFTW, un cahier de laboratoire en ligne et collaboratif p. 72
WIFI / SÉCURITÉ
CRÉEZ VOTRE HOTSPOT WIFI SÉCURISÉ CHEZ VOUS OU EN ENTREPRISE
p. 46
TUTORIELS
BUREAUTIQUE
Modifiez et créez vos propres polices à l'aide de FontForge p. 14
AUDIO
Réalisez vos enregistrements audio en toute simplicité avec Audio-Recorder p. 08
RED HAT / CENTOS
Bien configurer votre réseau et le dépanner avec les bons outils en cas de problème p. 62
ENTREPRISE
Le RGPD expliqué aux informaticiens
p. 80

6 MAGAZINES/AN

39€*

au lieu de 47,40 €

FRAIS DE PORT OFFERTS

*Prix TTC en Euros / France Métropolitaine

6X

Offre LP1

39€*

Prix kiosque : 47,40 €

Économie : 8,40 €

*Prix TTC en Euros / France Métropolitaine

6X

+

3X

Offre LP+1

69€*

Prix kiosque : 92,10 €

Économie : 23,10 €

*Prix TTC en Euros / France Métropolitaine

BULLETIN D'ABONNEMENT

☐ JE M'ABONNE À
LINUX PRATIQUE
6 numéros pour 39 €*

☐ JE M'ABONNE À
LINUX PRATIQUE ET SES HORS-SÉRIES
6 numéros et 3 hors-séries pour 69 €*

*Prix TTC en Euros / France Métropolitaine
Les tarifs hors France Métropolitaine, Europe, Asie, etc. sont disponibles en ligne !

À découper ou recopier et à renvoyer avec votre réglement à :

Les Éditions Diamond
Service des Abonnements
10, Place de la Cathédrale
68000 Colmar – France

JE RÈGLE ..... €

☐ par **chèque bancaire** ou **postal** à l'ordre des Éditions Diamond (uniquement France et DOM TOM)

☐ Pour les règlements par **virement**, veuillez nous contacter
par e-mail :
cial@ed-diamond.com
ou par téléphone :
+33 (0)3 67 10 00 20

COORDONNÉES DE L'ABONNÉ

Société : .....
Nom : .....
Prénom : .....
Adresse : .....
.....
Code Postal : .....
Ville : .....
Pays : .....
Téléphone : .....
E-mail : .....

☐ J'autorise Linux Pratique à me contacter par e-mail ou par téléphone

RETROUVEZ TOUTES NOS OFFRES SUR : www.ed-diamond.com !

CONSULTEZ EN NUMÉRIQUE !

...CELUI D'AUJOURD'HUI ET CEUX D'HIER...

...LE BIMESTRIEL ET LES HORS-SÉRIES !

RENDEZ-VOUS SUR :

connect.ed-diamond.com

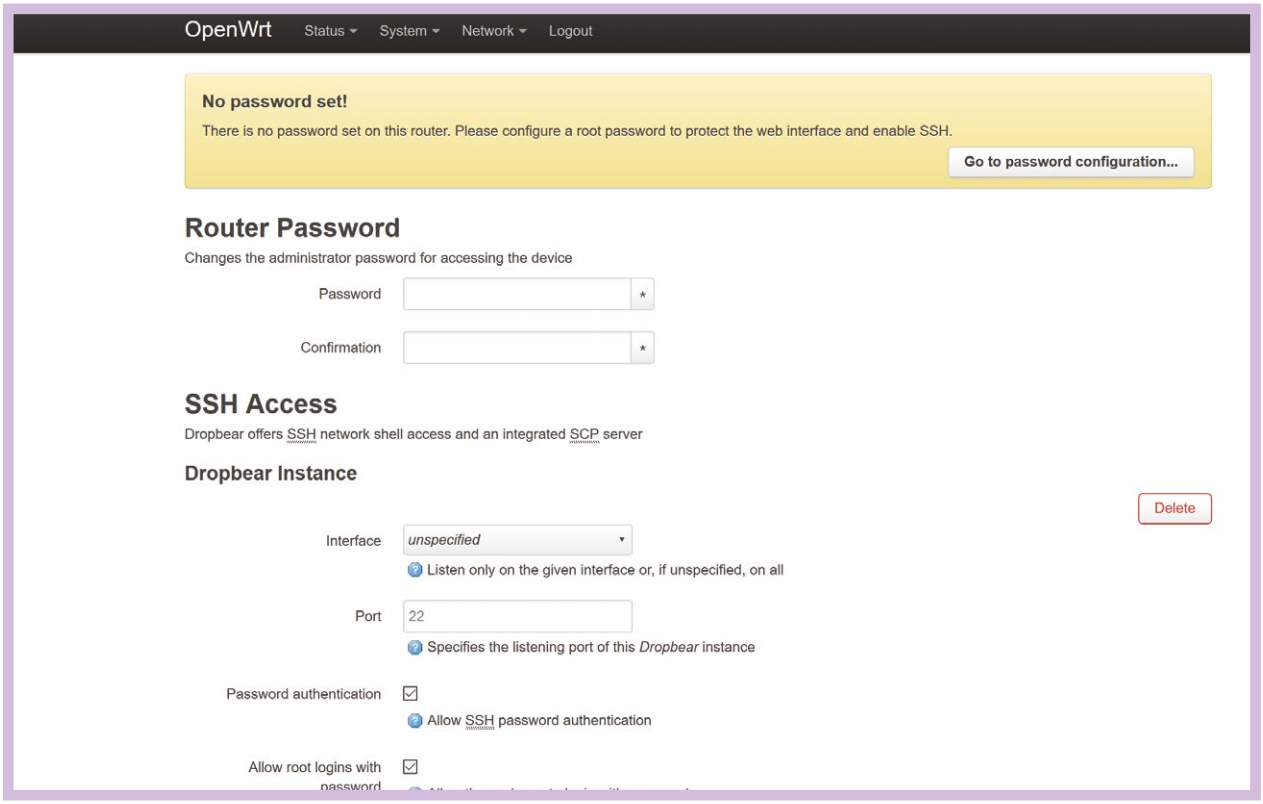


FIGURE 12. Accueil OpenWRT.

```
ngreneche@DESKTOP-RE130IB:~$ ssh
root@192.168.0.1
root@OpenWrt:~# cat /,etc/config/network

config interface 'lan'
        option type 'bridge'
        option ifname 'eth0.1'
        option proto 'static'
        option ipaddr '192.168.0.1'
        option netmask '255.255.255.0'
        option ip6assign '60'
```

Une fois le paramètre option ipadddr modifié de 192.168.1.1 vers 192.168.0.1, redémarrez OpenWRT :

```
root@OpenWrt:~# reboot
```

Pour en finir avec le LAN, il faut bien vérifier que le DHCP est activé. Retournez dans l'interface web d'OpenWRT et cliquez sur ***Network*** puis ***Interfaces*** et enfin, sur ***Edit*** de l'interface LAN. Vérifiez que le paramètre ***Ignore interface*** de

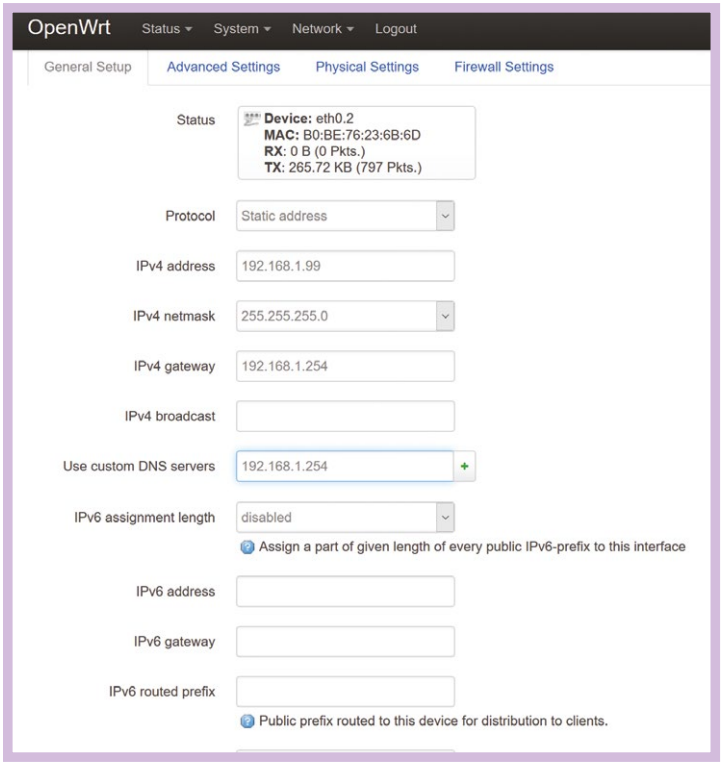


FIGURE 13. Configuration WAN d'OpenWRT.

l'onglet ***DHCP Server*** soit bien décoché. Faites également un tour dans la section ***Advanced Settings*** du serveur DHCP pour ajouter les options suivantes : « 6,192.168.1.254 » et « 3,192.168.0.1 ». En effet, pour DHCP chaque option supplémentaire passée au client correspond à un numéro qui préfixe l'adresse IP. Ainsi, nous avons l'option 6 qui définit le DNS et l'option 3 la passerelle par défaut à passer au client obtenant le bail. Dans certaines versions d'OpenWRT, les champs sont présentés explicitement.

Pour l'interface WAN, nous pouvons y aller sans soucis par l'interface web. À l'instar de pfSense, il faut juste lui définir une IP, un masque, une route par défaut et un serveur DNS. Cliquez sur ***Network*** puis ***Interfaces*** et enfin sur ***Edit*** de l'interface WAN. Vous allez tomber sur l'écran présenté en figure 13, page précédente. Vous pouvez maintenant raccorder le WAN au commutateur du réseau 192.168.1.0/24.

Vous pouvez y appliquer une configuration en adresse statique (***Protocol = Static Address***) avec l'IP 192.168.1.99 (***IPv4 address***), le masque à 255.255.255.0 (***IPv4 netmask***), la passerelle par défaut (***IPv4 gateway***) et le DNS (***Use custom DNS servers***) à 192.168.1.254. Comme d'habitude, on applique et on sauve. À partir de ce moment, les clients connectés en filaire à la borne TP-Link devraient pouvoir se connecter au monde extérieur. On notera que nous n'avons pour l'instant défini aucun réseau sans fil. C'est volontaire !

2.3 Installation et configuration de FreeRadius

Pour faire très très simple, Radius et un protocole d'authentification populaire dans le monde des appliances réseau, car il est simple, donc peu gourmand en ressources. Nous allons installer l'implémentation FreeRadius sur notre borne OpenWRT. Pour ce faire, ouvrons une session SSH :

```
ngreneche@DESKTOP-RE130IB:~$ ssh root@192.168.0.1
```

Et utilisons le gestionnaire de paquets d'OpenWRT opkg :

```
root@OpenWrt:~# opkg update
root@OpenWrt:~# opkg install freeradius3 freeradius3-common
freeradius3-democerts freeradius3-mod-always freeradius3-
mod-attr-filter freeradius3-mod-chap freeradius3-mod-detail
freeradius3-mod-digest freeradius3-mod-eap freeradius3-mod-
eap-gtc freeradius3-mod-eap-leap freeradius3-mod-eap-md5
freeradius3-mod-eap-mschapv2 freeradius3-mod-eap-peap
freeradius3-mod-eap-tls freeradius3-mod-eap-ttls freeradius3-
mod-exec freeradius3-mod-expiration freeradius3-mod-expr
freeradius3-mod-files freeradius3-mod-logintime freeradius3-
mod-mschap freeradius3-mod-pap freeradius3-mod-preprocess
freeradius3-mod-radutmp freeradius3-mod-realm freeradius3-mod-
unix freeradius3-utils
```

L'update permet de mettre à jour l'index des paquets et install de les installer. On voit qu'il y en a un paquet à installer ! En fait, cela s'explique par le fonctionnement de Radius. En général, on a un serveur Radius central adossé au système d'authentification (OpenLDAP, Active Directory, etc.) et des petits systèmes satellites autour qui interrogent ce système central. Typiquement, les systèmes embarquant OpenWRT sont plutôt destinés à être des satellites. Donc FreeRadius a été saucissonné en petits modules pour satisfaire les besoins des satellites de façon unitaire.

Examinons maintenant la configuration du serveur FreeRadius :

```
root@OpenWrt:~# cat /etc/freeradius3/clients.conf | egrep -v
"^\s*(#|$)"
client localhost {
        ipaddr = 127.0.0.1
        proto = *
        secret = testing123
        require_message_authenticator = no
        nas_type      = other
        limit {
                max_connections = 16
                lifetime = 0
                idle_timeout = 30
        }
}
```

Cette directive client définit les sources autorisées à tenter une authentification. Ici, on n'accepte qu'une source locale (*localhost*). Cette directive crée un point d'entrée destiné aux satellites pour réaliser les authentifications qu'on leur demande. Si on examine le point d'entrée nommé localhost, on constate qu'il y a deux attributs particulièrement significatifs :

ipaddr et secret. ipaddr spécifie l'adresse sur laquelle FreeRadius attend les authentifications et secret est un mot de passe qui doit être renseigné dans la configuration du satellite pour qu'il puisse s'adresser au serveur FreeRadius.

Dans notre cas, c'est la borne OpenWRT elle-même qui va faire office de serveur FreeRadius. Il va donc falloir :

1) créer un utilisateur ;

2) configurer l'accès au serveur FreeRadius local.

Pour créer l'utilisateur, nous allons utiliser la méthode la plus simple, à savoir déclarer un identifiant et un mot de passe en clair dans un fichier plat. Cela se passe dans le fichier /etc/freeradius3/mods-config/files/authorize.

```
root@OpenWrt:~# cat /etc/freeradius3/mods-config/files/authorize
nico Cleartext-Password := "Deftones"
```

Nous avons créé un utilisateur nico qui utilise la méthode d'authentification mot de passe en clair (Cleartest-Password) avec comme mot de passe Deftones.

Pour l'accès au FreeRadius, la philosophie des réseaux sans fil est la suivante : une méthode d'authentification est attachée à un SSID. Pour prendre un exemple concret, lorsque vous êtes abonné chez Free, vous avez deux SSID : un personnel pour votre box et un autre nommé *freewifi*. Le premier s'appuie sur un mécanisme PSK (*Pre-Shared Key*), c'est-à-dire que vous devez entrer une longue phrase qui fait office de secret entre vous et la box. Pour le *freewifi*, vous avez un identifiant et un mot de passe. Nous allons donc créer notre SSID s'authentifiant en 802.1X sur notre serveur FreeRadius :

```
root@OpenWrt:~# cat /etc/config/wireless
config wifi-iface
        option device 'radio1'
        option mode 'ap'
        option ssid 'OpenWrt _ 8021X'
        option network 'lan'
        option encryption 'wpa2'
        option server '127.0.0.1'
        option key 'testing123'
```

Les trois attributs les plus significatifs sont ssid qui définit le nom de notre nouveau SSID, server qui pointe sur le serveur RADIUS à interroger (ici, le local 127.0.0.1) et key qui est le mot de passe associé. Vous retrouvez bien les paramètres de la configuration du serveur. Les clients voulant s'attacher à ce réseau Wi-Fi vont se voir demander un identifiant et un mot de passe au moment de se connecter au SSID OpenWrt_8021X.

CONCLUSION

Dans cet article, nous avons abordé le portail captif qui est un moyen simple d'authentifier les utilisateurs avant leur sortie sur Internet. Son utilisation nécessite juste la présence d'un navigateur web sur la machine. Cependant, pour accéder au portail la machine doit disposer d'un minimum de connectivité (ne serait-ce qu'un accès au serveur DNS). En complément, et j'insiste sur le mot complément, car les deux méthodes ne s'opposent pas, nous pouvons aussi utiliser le 802.1X. Comme l'authentification est déportée sur l'équipement de commutation, c'est donc une connaissance d'un secret qui conditionne l'accès physique au réseau. De plus, nous n'avons fait qu'effleurer les possibilités du 802.1X qui sert de base à des mécanismes comme l'assignation dynamique dans des VLANs ou encore des contrôles de conformité sur la machine avant tout accès au réseau, etc. Nous avons la possibilité de proposer deux SSID : un relié au portail captif et l'autre au réseau 802.1X. ■

RÉFÉRENCES

[1] https://www.pc2s.fr/pfsense-installation-et-configuration

[2] https://connect.ed-diamond.com/GNU-Linux-Magazine/GLMF-198/Les-reseaux-logiques-VLANs

[3] https://connect.ed-diamond.com/GNU-Linux-Magazine/GLMF-175/Introduction-au-Network-Security-Monitoring-NSM

[4] https://openwrt.org/_media/toh_dump_tab_separated_csv.csv.gz

[5] http://downloads.openwrt.org/releases/18.06.2/targets/ar71xx/generic/openwrt-18.06.2-ar71xx-generic-archer-c7-v5-squashfs-factory.bin

OPTIMISER LES CONNEXIONS RÉSEAUX sous CentOS/RHEL 7

ISSAM MEJRI

DANS CET ARTICLE, ON AURA L'OCCASION DE PLONGER EN PROFONDEUR DANS LA CONFIGURATION RÉSEAU DES MACHINES SOUS CENTOS 7 / RHEL 7. LET'S GET STARTED !

INTRODUCTION

ARPANET (*Advanced Research Projects Agency Network*) est un projet fondé aux États-Unis par la DARPA, une agence du département de la défense chargée de mettre en place des solutions technologiques de pointe dédiées exclusivement à des usages militaires. Ce projet vise à créer un réseau à transfert de paquets qui est devenu aujourd'hui ce que nous appelons Internet.

Et depuis tout l'univers a changé, toutes nos perceptions à la manière de gérer notre quotidien a également changé ; pensez par exemple à ce que vous pouvez faire avec votre smartphone aujourd'hui.

Bref, le sujet du réseau est important donc, sans Internet, sans communication, rien ne pourra fonctionner, c'est quelque chose de vital presque au même degré que l'eau ou l'oxygène que nous respirons.

Dans un contexte purement technique, une mauvaise configuration réseau pourra mettre un système

en état de dysfonctionnement, provoquant une mise hors ligne d'un ensemble de services. Les fournisseurs cloud aujourd'hui prennent en charge toute la partie réseau pour leurs clients ainsi que la partie hardware et OS, on parle de l'offre de service IAAS (*Infrastructure As A Service*), vous permettant de déléguer une partie de l'administration de cette couche d'infrastructure à la charge du *Provider Cloud*. Mais lorsque vous gérez vos propres serveurs dans vos centres de données, il faut être en mesure de configurer, d'optimiser et de paramétrer finement leur partie Networking.

1. RAPPEL SUR LE NETWORKMANAGER

Sous les distributions GNU/Linux CentOS 7 / RHEL 7, la configuration des interfaces réseau est gérée par un service appelé le NetworkManager. Dans le NetworkManager, on aura un périphérique qui est une interface réseau.

Une connexion est un ensemble de paramètres qu'il est possible de configurer pour un périphérique. Un périphérique n'accepte qu'une seule connexion active. Des connexions multiples peuvent exister pour être utilisées par plusieurs périphériques ou pour permettre de modifier la configuration d'un même périphérique. Chaque connexion est identifiée par son nom ou encore par son ID.

Pour la persistance des connexions, celles-ci seront enregistrées dans le fichier /etc/sysconfig/network-scrtipts/ifcfg-nom-de-connexion où le nom-connexion est le nom donné à la connexion réseau créée. Il est également possible d'éditer ce fichier manuellement. L'utilitaire nmcli permet de créer et de modifier les fichiers de connexions à partir de l'invite du shell.

Dans la suite de l'article, nous utilisons la distribution CentOS 7. Cette instance est déployée sur le cloud Provider DigitalOcean et aura une adresse IP publique.

1.1 Affichage des informations réseau

La commande nmcli dev status affiche l'état de tous les périphériques réseau :

```
[root@centos-7 ~]# nmcli dev status
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  eth0
eth1    ethernet  connected  eth1
lo      loopback  unmanaged  --
```

La commande nmcli con show affiche la liste de toutes les connexions. Pour afficher uniquement les connexions actives, ajoutez l'option --active :

```
[root@centos-7 ~]# nmcli con show
NAME         UUID                                   TYPE      DEVICE
eth0         985b4978-7872-42bc-b30a-0b12664bf2a7   ethernet  eth0
eth1         6fc4857c-d2ed-48c9-9a61-c949bd94c35d   ethernet  eth1
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03   ethernet  --
System eth1  9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04   ethernet  --
```

Pour afficher uniquement les connexions actives :

```
[root@centos-7 ~]# nmcli dev status --active
Unknown parameter: --active
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  eth0
eth1    ethernet  connected  eth1
lo      loopback  unmanaged  --
```

La commande ip addr show affiche la configuration actuelle des interfaces réseau sur le système. Pour afficher une seule interface, ajoutez le nom de l'interface comme dernier argument :

```
[root@centos-7 ~]# ip add show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_
fast state UP group default qlen 1000
    link/ether 0a:2d:23:a7:e4:ee brd ff:ff:ff:ff:ff:ff
    inet 104.248.127.11/20 brd 104.248.127.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.10.0.6/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2604:a880:400:d1::bcd:5001/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::82d:23ff:fea7:e4ee/64 scope link
       valid_lft forever preferred_lft forever
```

Pour résumer les informations affichées par cette commande :

- Une interface active est UP.
- La ligne link/ether spécifie l'adresse matérielle (MAC) du périphérique.
- La ligne inet présente une adresse IPv4, la longueur du préfixe et l'étendue de son réseau.
- La ligne inet6 présente une adresse IPv6, la longueur du préfixe et l'étendue de son réseau.

1.2 Ajout d'une connexion réseau

La commande nmcli con add permet d'ajouter de nouvelles connexions réseau.

La commande qui suit ajoutera une nouvelle connexion à l'interface eth0 qui obtiendra alors les informations sur le réseau IPv4 en utilisant le protocole DHCP et se connectera automatiquement au démarrage. La configuration sera enregistrée dans /etc/sysconfig/network-scripts/ifcfg-diamond, car le nom attribué à la connexion sera diamond.

```
[root@centos-7 ~]# nmcli con add con-name
diamond type ethernet ifname eth0
Connection 'diamond' (eead0872-f752-4d34-
b176-63b23471e8ea) successfully added.
```

La fichier /etc/sysconfig/network-scripts/ifcfg-diamond sera créé comme suit :

```
TYPE=Ethernet
PROXY _ METHOD=none
BROWSER _ ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4 _ FAILURE _ FATAL=no
IPV6INIT=yes
IPV6 _ AUTOCONF=yes
IPV6 _ DEFROUTE=yes
IPV6 _ FAILURE _ FATAL=no
IPV6 _ ADDR _ GEN _ MODE=stable-privacy
NAME=diamond
UUID=eead0872-f752-4d34-b176-63b23471e8ea
DEVICE=eth0
ONBOOT=yes
```

La configuration statique de la connexion se fait de la même manière en ajoutant quelques paramètres liés à l'adressage et au routage :

```
[root@centos-7 network-scripts]# nmcli con
add con-name diamond type ethernet ifname
eth0 ip4 192.168.0.5/24 gw4 192.168.0.254
Connection 'diamond' (e88b9f9a-a4ff-4c3d-
aec5-a9fde688deca) successfully added.
```

Vérifions une autre fois le contenu du script de configuration réseau :

```
TYPE=Ethernet
PROXY _ METHOD=none
BROWSER _ ONLY=no
BOOTPROTO=none
IPADDR=192.168.0.5
PREFIX=24
GATEWAY=192.168.0.254
DEFROUTE=yes
IPV4 _ FAILURE _ FATAL=no
IPV6INIT=yes
IPV6 _ AUTOCONF=yes
IPV6 _ DEFROUTE=yes
IPV6 _ FAILURE _ FATAL=no
IPV6 _ ADDR _ GEN _ MODE=stable-privacy
NAME=diamond
UUID=e88b9f9a-a4ff-4c3d-aec5-a9fde688deca
DEVICE=eth0
ONBOOT=yes
```

1.3 Contrôle des connexions réseau

La commande nmcli con up/down name activera/désactivera la connexion name sur l'interface réseau à laquelle elle est liée. Notez que la commande prend le nom d'une connexion, et non le nom de l'interface réseau.

Vérifions tout d'abord les connexions actives :

```
[root@centos-7 ~]# nmcli con show --active
NAME          UUID
TYPE      DEVICE
System eth0   5fb06bd0-0bb0-7ffb-45f1-
d6edd65f3e03  ethernet  eth0
System eth1   9c92fad9-6ecb-3e6c-eb4d-
8a47c6f50c04  ethernet  eth1
```

Mettons la connexion System eth0 hors service :

```
[root@centos-7 ~]# nmcli con down "System
eth0"
```

Pour réactiver la connexion :

```
[root@centos-7 ~]# nmcli con up "System
eth0"
```

La commande nmcli dev disconnect device déconnectera l'interface réseau périphérique et l'arrêtera. Cette commande peut être abrégée en nmcli dev dis device :

```
root@centos-7 ~]# nmcli dev dis eth0
```

» REMARQUE

En général, la commande nmcli con down name ne constitue pas le meilleur moyen de désactiver une interface réseau. Cette commande coupera la connexion. Cependant, la plupart des connexions systèmes câblées sont configurées par défaut avec l'option autoconnect activée. Cette option active la connexion dès que son interface réseau est disponible. Étant donné que l'interface réseau de la connexion est toujours disponible, la commande nmcli con down name arrête l'interface, mais NetworkManager la réactive immédiatement après, à moins que la connexion ne soit complètement déconnectée de l'interface.

1.4 Modification des paramètres de connexion réseau

Les connexions NetworkManager présentent deux types de paramètres. Il existe des propriétés de connexion statiques, qui sont configurées par l'administrateur et enregistrées dans le fichier de configuration présent dans /etc/sysconfig/network-scripts/ifcg-*. Il peut également y avoir des données de connexions actives que la connexion extrait d'un serveur DHCP, mais qui ne sont pas enregistrées de manière persistante.

Une autre commande également très utile permettant de modifier à chaud les paramètres d'une connexion est la commande nmcli con mod name. Cette commande agit en conséquence sur le fichier de configuration de la connexion en question. La modification peut affecter plusieurs paramètres, tels que l'adressage, la passerelle par défaut, les serveurs de nom DNS.

Pour afficher la liste des paramètres actuels d'une connexion, exécutez la commande nmcli con show où name est le nom de la connexion. Les paramètres en minuscules sont les propriétés statiques modifiables par l'administrateur, tandis que les paramètres en majuscules sont les paramètres actifs utilisés temporairement pour l'instance de la connexion.

```
[root@centos-7]# nmcli con show eth0
```

```
connection.id:
eth0
connection.uuid:
95edbf2e-f16e-42e4-95df-cbc4cc442de1
connection.stable-id:                   --
connection.type:
802-3-ethernet
connection.interface-name:
eth0
connection.autoconnect:                 no
connection.autoconnect-priority:        0
connection.autoconnect-retries:         -1
(default)
connection.auth-retries:                -1
connection.timestamp:
1556464768
connection.read-only:                   no
connection.permissions:                 --
connection.zone:                        --
connection.master:                      --
connection.slave-type:                  --
connection.autoconnect-slaves:          -1
(default)
********   Affichage tronqué ***********
```

La commande nmcli con mod name permet de modifier les paramètres d'une connexion.

Ces modifications sont également enregistrées dans le fichier /etc/sysconfig/network-scripts/ifcfg-name de la connexion.

Voici un exemple : pour définir l'adresse IPv4 sur 192.168.2.2/24 et la passerelle par défaut sur 192.168.2.254 pour la connexion eth1, on passe la commande suivante :

```
[root@ centos-7]# nmcli con mod eth0 ipv4.
addresses  ''192.168.2.2/24  192.168.2.254/24''
```

Remarque : il important de savoir que dans la commande précédente, eth0 représente le nom de la connexion et non pas le nom de l'interface.

Un certain nombre de paramètres peuvent accepter plusieurs valeurs. Il est possible d'ajouter ou de supprimer une valeur spécifique à une liste ou à un paramètre en ajoutant un signe + ou - devant le nom du paramètre.

Pour ajouter le serveur DNS 192.168.2.1 à la liste des serveurs de noms à utiliser avec la connexion eth0 :

```
[root@centos-7]# nmcli con mod eth0 +ipv4.
dns 192.168.2.1
```

Par défaut, les modifications effectuées avec la commande nmcli con mod name sont automatiquement enregistrées dans etc/sysconfig/network-scripts/ifcfg-name.

Pour la configuration des serveurs DNS, il faut savoir que toutes modifications directes du fichier /etc/resolv.conf risquent d'être écrasées, car le NetworkManager a tendance à modifier automatiquement ce fichier.

1.5 Modification du nom d'hôte du système

La commande hostname affiche ou modifie temporairement le nom d'hôte entièrement qualifié du système.

```
[root@centos-7]# hostname
centos-7
```

Un nom d'hôte statique peut être spécifié dans le fichier /etc/hostname. La commande hostnamectl sert à modifier ce fichier et peut être utilisée pour afficher l'état du nom d'hôte entièrement qualifié du système. Si le fichier n'existe pas, le nom d'hôte est défini par une requête DNS inverse une fois qu'une adresse IP est attribuée à l'interface.

La commande hostnamectl affiche plus d'informations que hostname tel que le système de virtualisation utilisé, la version du noyau Linux et l'architecture :

```
[root@centos-7]# hostnamectl
Static hostname: centos-7
         Icon name: computer-vm
           Chassis: vm
        Machine ID:
0bb0dd0c6b2af818a78281505cb4c536
           Boot ID:
3bc2333c994943dc9cae5afc5a9b0cd0
    Virtualization: kvm
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-957.1.3.el7.
x86 _ 64
      Architecture: x86-64
```

2. DÉPANNAGE RÉSEAU

Le risque d'avoir des problèmes de connectivité est très probable, donc il faut savoir utiliser des outils et des utilitaires dédiés pour la résolution des problèmes qui surviennent sur le réseau.

L'utilitaire le plus utilisé est la commande ping ; cette commande permet de tester si une machine est joignable ou non.

```
[root@centos-7 ~]# ping 10.136.198.13
PING 10.136.198.13 (10.136.198.13) 56(84)
bytes of data.
64 bytes from 10.136.198.13: icmp _ seq=1
ttl=64 time=0.016 ms
64 bytes from 10.136.198.13: icmp _ seq=2
ttl=64 time=0.037 ms
64 bytes from 10.136.198.13: icmp _ seq=3
ttl=64 time=0.028 ms
```

Dans cet exemple, la commande ping renvoie une réponse, donc l'hôte est joignable et le temps de réponse est acceptable (time=0.016 ms). La réponse est un Echo Reply via des requêtes ICMP.

Maintenant essayons de pinger une deuxième machine avec le nom d'hôte :

```
[root@centos-7 ~]# ping  host.lan.local
ping: host.lan.local: Name or service not
known
```

Ici, plusieurs cas sont envisageables :

1. l'hôte est inexistant ;
2. la machine locale n'arrive pas à joindre l'hôte distant ;
3. problème de résolution du nom d'hôte vers l'adresse IP ;
4. problème de routage.

Au cas par cas :

1. L'hôte est inexistant : il se peut que l'hôte concerné soit inexistant sur le réseau ou que le nom d'hôte soit modifié, dans ce cas, il faut exécuter des commandes adéquates pour vérifier la résolution DNS :

```
[root@centos-7]# dig host.lan.local
 <<>> DiG 9.9.4-RedHat-9.9.4-73.el7 _ 6 <<>> host.lan.
local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id:
15160
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0,
AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;host.lan.local.                        IN      A
;; AUTHORITY SECTION:
.                       891     IN      SOA     a.root-
servers.net. nstld.verisign-grs.com. 2019042800 1800
900 604800 86400
;; Query time: 4 msec
;; SERVER: 67.207.67.3#53(67.207.67.3)
;; WHEN: Sun Apr 28 16:41:10 UTC 2019
;; MSG SIZE  rcvd: 118
```

On remarque que le serveur DNS interrogé est le 67.207.67.3 et est donc accessible, mais aucun enregistrement n'existe dans la zone DNS pour l'entrée demandée. On peut conclure que l'hôte n'existe pas ou qu'il existe et que l'entrée n'est pas encore introduite dans les fichiers de zones de la configuration du serveur DNS. Dans ce cas, il faut contacter l'administrateur du serveur DNS.

2. La machine locale n'arrive pas à joindre l'hôte distant : il faut vérifier que le réseau est correctement configuré sur la machine locale et que l'interface à partir de laquelle on effectue des requêtes et en UP.

On commence par une manipulation simple avec la commande ip address show :

```
[root@centos-7]# ip address show
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether f6:11:f1:f0:5d:8c brd ff:ff:ff:ff:ff:ff
    inet 142.93.10.62/20 brd 142.93.15.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.10.0.5/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2604:a880:400:d1::815:1/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::f411:f1ff:fef0:5d8c/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether 46:71:69:2c:4a:32 brd ff:ff:ff:ff:ff:ff
    inet 10.136.198.13/16 brd 10.136.255.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::4471:69ff:fe2c:4a32/64 scope link
       valid_lft forever preferred_lft forever
```

On constate que l'interface eth0 ayant l'adresse 142.93.10.62 est UP et c'est la même chose pour l'interface eth1, donc pas de soucis avec la configuration du réseau local.

Problème de résolution du nom d'hôte vers l'adresse IP : il faut s'assurer que votre machine puisse traduire l'adresse host.lan.local en adresse IP correspondante. Pour cela, il faut vérifier le contenu du fichier résolveur /etc/resolv.conf et que vous puissiez joindre le serveur DNS en question.

```
[root@centos-7]# vim /etc/resolv.conf
```

```
; Created by cloud-init on instance boot automatically, do not edit.
;
nameserver 67.207.67.3
nameserver 67.207.67.2
```

```
[root@centos-7]# ping 67.207.67.3
PING 67.207.67.3 (67.207.67.3) 56(84) bytes of data.
64 bytes from 67.207.67.3: icmp_seq=1 ttl=61 time=0.837 ms
64 bytes from 67.207.67.3: icmp_seq=2 ttl=61 time=0.289 ms
```

Le serveur DNS est joignable et le résolveur est bien configuré, donc cette piste est éliminée.

3. Problème de routage : il est possible que votre machine en local ne puisse pas accéder à l'extérieur via la passerelle par défaut ou via les routes existantes, les commandes ip route et traceroute sont dans ce cas envisageables :

```
[root@centos-7 ~]# ip route
default via 142.93.0.1 dev eth0
10.10.0.0/16 dev eth0 proto kernel scope
link src 10.10.0.5
10.136.0.0/16 dev eth1 proto kernel scope
link src 10.136.198.13
142.93.0.0/20 dev eth0 proto kernel scope
link src 142.93.10.62
169.254.0.0/16 dev eth0 scope link metric
1002
169.254.0.0/16 dev eth1 scope link metric
1003
```

On remarque que la passerelle par défaut est 142.93.0.1, en effectuant un traceroute vers la passerelle :

```
[root@centos-7 ~]# traceroute 142.93.0.1
traceroute to 142.93.0.1 (142.93.0.1), 30 hops
max, 60 byte packets
 1  gateway (142.93.0.1)  1.214 ms  3.537 ms
2.029 ms
```

On remarque sur la sortie de la commande que notre passerelle est le premier routeur sur lequel la machine est connectée et qu'il est joignable également, donc pas de soucis au niveau du routage.

Dans cet exemple, je voulais juste vous donner la marche à suivre lorsqu'il s'agit de diagnostiquer les problèmes réseaux qui peuvent survenir, et principalement lorsqu'une machine qui peut être un serveur web, FTP ou autres ressource sur le réseau. Il faut commencer par vérifier la configuration en local puis inspecter les différentes connectivités vers le ou les réseaux cibles.

CONCLUSION

L'optimisation et une bonne configuration réseau d'un serveur sont primordiales pour la continuité du service. Dans cet article j'ai évoqué les bases pour configurer correctement le réseau sous CentOS 7. D'autres techniques existent pour l'optimisation et la haute disponibilité, à savoir l'association réseau et les ponts réseaux qui seront abordés dans un prochain article. ■

ACTUELLEMENT DISPONIBLE !

MISC n°104

MISC
LE MAGAZINE DE LA CYBERSÉCURITÉ OFFENSIVE ET DÉFENSIVE
N° 104
JUILLET / AOÛT 2019
SYSTÈME : RÉSEAUX SOCIAUX / OSINT
Découvrez les outils de recueil et d'analyse des informations sur les réseaux sociaux
RÉSEAU : SDR / DÉCODAGE
Analyse et interception de flux des téléphones satellites Iridium
ORGANISATION : NORMES / ISO 27001
La gestion des incidents de sécurité selon la norme ISO 27035
DOSSIER
MASQUEZ VOS ATTAQUES
POUR BIEN RÉUSSIR VOS MISSIONS RED TEAM
1 - De la reconnaissance à la post-exploitation : comment rester furtif
2 - Techniques pour déjouer les mécanismes de sécurité de PowerShell
3 - Scripts malveillants sur Windows 10 : fonctionnement et contournements d'AMSI
EXPLOIT CORNER
Élévation de privilèges Windows avec CVE 2018-0977
PENTEST CORNER
Détecter des vulnérabilités exploitables avec Fuddly
IOT CORNER
Prise de contrôle à distance d'un drone

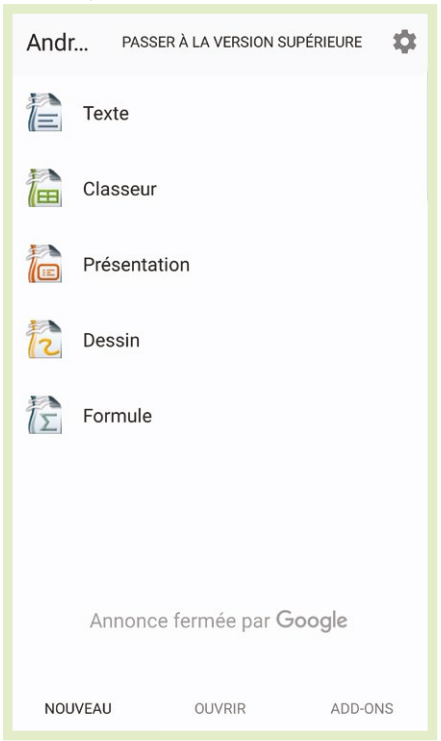
MASQUEZ VOS ATTAQUES
POUR BIEN RÉUSSIR VOS MISSIONS RED TEAM

NE LE MANQUEZ PAS
CHEZ VOTRE MARCHAND DE JOURNAUX ET SUR :
https://www.ed-diamond.com

ANDROPEN OFFICE

RETROUVEZ UNE SUITE BUREAUTIQUE SUR MOBILE

AndrOpen Office se présente comme une version déclinée (non officielle) d'Open Office sur mobile et tablette. Elle vous permettra ainsi de profiter des outils de la suite bureautique où que vous soyez avec un traitement de texte, un tableur, un logiciel de présentation, de dessin et un éditeur de formules (autrement dit, les « équivalents » de Writer, Calc, Impress, Draw et Math).



Comme sa version desktop, de nombreux formats de fichiers sont également supportés ici et les options incontournables des outils bureautiques sont au rendez-vous. Depuis la page d'accueil, on pourra créer un nouveau document à l'aide de l'outil de son choix, ouvrir un fichier présent sur son appareil ou compléter les fonctionnalités proposées par l'ajout d'add-ons (nouvelles polices, pack français ou encore pack pro payant permettant de passer à une version supérieure de l'application plus complète sans publicités…).

Les principales options des différents éditeurs sont facilement accessibles entre la barre de menu du haut de l'interface et celle du bas avec ses icônes. On trouvera également tout en bas une barre d'état supplémentaire fournissant un menu principal regroupant toutes les fonctionnalités de l'outil, un outil de recherche, un pavé numérique, un simulateur de souris et évidemment un clavier qu'on activera avant de vouloir rédiger quoi que ce soit. Ce sont de petites habitudes à prendre et il faudra évidemment faire avec le format de son appareil qui ne rend pas toujours la prise en main aisée. AndrOpen Office constitue cependant un bon outil d'appoint pour retrouver ses habitudes bureautiques sur mobile. ■

SITE : https://andropenoffice.blogspot.com/

VERSION TESTÉE : 4.3

PRIVATE BROWSER ET NAVIGATION INCOGNITO

UNE NAVIGATION PRIVÉE ET ANONYME

Développé entre autres par Adblock, Private Browser et Navigation incognito est un navigateur web pour mobile qui se veut vous offrir anonymat et protection contre le pistage lors de vos explorations sur la Toile. Pour atteindre ces promesses, l'application compte au nombre de ses fonctionnalités un bloqueur de publicités que vous pourrez choisir d'activer ou non en fonction des sites que vous visitez. Le comportement de ce dernier est paramétrable depuis les options du navigateur.

Rechercher ou saisir une l
Vous êtes passé en mode navigation privée
Les pages consultées dans les onglets de navigation privée ne sont pas enregistrées dans l'historique de votre navigateur, dans les cookies ni dans l'historique des recherches une fois que vous avez fermé tous les onglets de navigation privée. Les fichiers téléchargés et les favoris ajoutés sont conservés.
Vous n'êtes cependant pas devenu invisible. L'utilisation du mode navigation privée n'empêche pas votre employeur, votre fournisseur d'accès à Internet ou les sites Web que vous avez consultés d'avoir accès aux informations relatives à votre navigation.

https://www.nytimes.com
Tech Giants Build a Lobbying Army for Battle With Washington
• Amazon, Apple, Facebook and Google
21
Pubs bloquées
0.19
Mo économisés
Bloqueur de pubs activé www.nytimes.co...
Problème avec le blocage de pubs sur ce site ?
SIGNALER UN PROBLÈME

Le navigateur propose par défaut un mode de navigation privé, comprenez par là que ni votre historique de recherche, ni vos cookies ne seront conservés. Vous pourrez cependant toujours ajouter des favoris ou enregistrer des fichiers. Au rang des autres options disponibles, on notera la possibilité de bloquer les demandes de notifications des sites, agrandir le texte pour permettre une lecture plus confortable, désactiver la collecte de données anonymes, activer les suggestions en cas d'erreur de navigation, bloquer les fenêtres pop-up, autoriser ou non les sites à exécuter JavaScript… L'application reste facilement configurable et simple à prendre en main pour pouvoir naviguer en toute tranquillité. ■

VERSION TESTÉE : 64.0.2016123125

SITE : https://play.google.com/store/apps/details?id=com.hsv.privatebrowser

ElabFTW, VOTRE CAHIER DE LABORATOIRE NUMERIQUE

ANTHONY CARRÉ

L'ENSEMBLE DES TRAVAUX SCIENTIFIQUES DES CHERCHEURS EST RETRANSCRIT DANS LEURS CAHIERS DE LABORATOIRE AFIN DE DÉTAILLER LES EXPÉRIENCES, LES THÉORIES, LES CONCLUSIONS. LE BUT EST À LA FOIS DE RENDRE LES RÉSULTATS COMPRÉHENSIBLES PAR D'AUTRES (OU SOI-MÊME), MAIS AUSSI DE RENDRE CEUX-CI OFFICIELLEMENT DATÉS. LA PLUPART DU TEMPS, LES LABORATOIRES UTILISENT DES CAHIERS EN PAPIER, MAIS LE BESOIN TOUJOURS GRANDISSANT DE COLLABORATION ET DE DONNÉES NUMÉRIQUES INCITE À MIGRER VERS DES SOLUTIONS LOGICIELLES.

eLabFTW est une application PHP/MySQL permettant à ses utilisateurs l'utilisation d'un cahier de laboratoire électronique collaboratif en ligne. Distribué sous licence libre AGPL, cet outil multiplateforme et gratuit est simple à prendre en main tout en proposant, en complément, des fonctionnalités particulièrement intéressantes : planificateur de réservation, gestionnaire d'inventaire, todo-list, etc.

Parmi les fonctionnalités importantes, on notera surtout l'horodatage des expériences conforme au standard RFC 3161, permettant de

prouver l'existence des entrées à une date donnée, ce qui peut être nécessaire pour gérer d'éventuelles questions de propriété intellectuelle.

1. INSTALLATION D'ELABFTW

L'installation peut se faire de différentes façons, mais la plus simple consiste à passer par une image Docker disponible pour architecture 64 bits. La procédure à suivre est largement détaillée dans la documentation officielle d'eLabFTW **[1]**.

Pour l'installation préalable de Docker, plusieurs solutions sont évidemment possibles : vous pouvez par exemple utiliser les paquets de votre distribution ou ajouter les dépôts spécifiques. Attention, les utilisateurs de Debian (et dérivés) souhaitant passer par leur gestionnaire de paquets sans ajouter de dépôts supplémentaires peuvent rencontrer une étrange difficulté : il existe un paquet docker, mais celui-ci est complètement hors propos (paquet de transition pour l'application de « dock » pour la zone de notification), pour l'installation de la plateforme de conteneurs c'est le paquet docker.io qu'il vous faudra installer.

À titre d'exemple, l'installation des dépendances d'eLabFTW sous Debian se fait donc ainsi :

```
apt install dialog git zip curl docker.
io docker-ce docker-ce-cli containerd.io
docker-compose
```

Après installation de Docker, vous devez ajouter votre utilisateur au groupe correspondant :

```
sudo gpasswd - a $USER docker
```

Cette dernière opération ne sera effective qu'une fois l'utilisateur déconnecté puis reconnecté.

Maintenant que les prérequis sont en place, l'installation d'eLabFTW se fait en quelques commandes simples :

```
curl - sL https://get.elabftw.net - o elabctl
chmod +x elabctl
mv elabctl /usr/local/bin/
elabctl install
```

La dernière commande exécute un script qui installera et configurera eLaFTW en quelques questions.

Vous pourrez constater que tout est fait pour inciter à la mise en place de certificat TLS (utilisation de https), si vous ne souhaitez pas une connexion sécurisée, cela compliquera fortement votre installation.

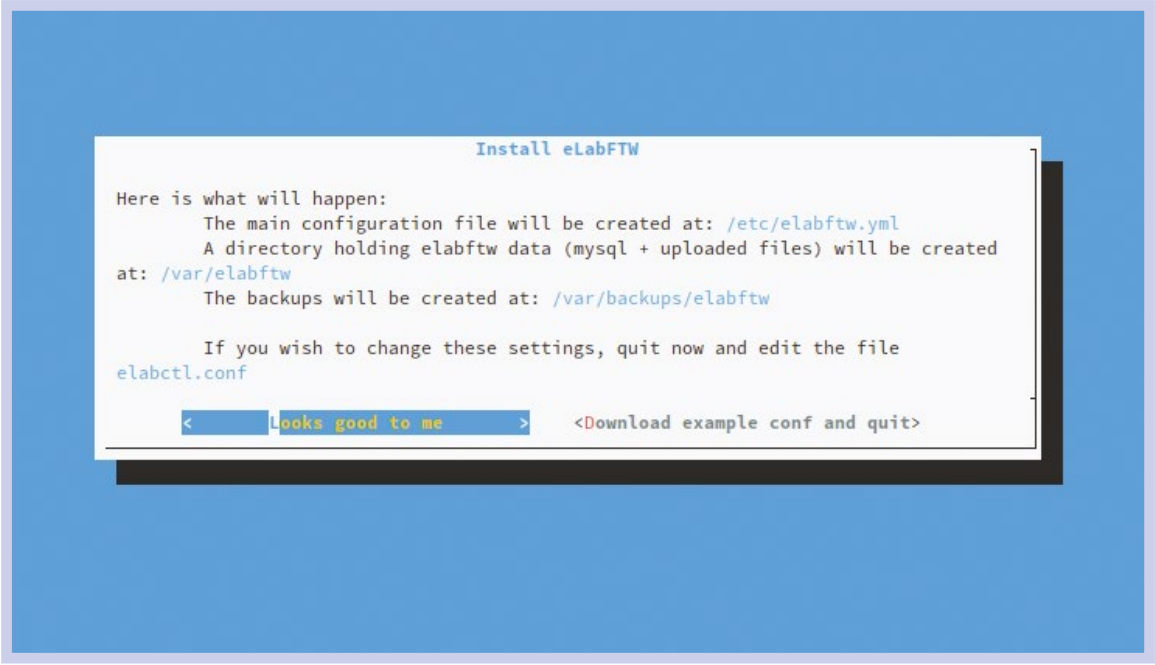


FIGURE 1. 5 ou 6 questions simples et c'est installé.

2. POST-INSTALLATION

Il ne reste plus que quelques étapes à suivre pour avoir une installation finalisée :

- configuration du serveur de mail (pour permettre la réinitialisation des mots de passe utilisateur au moins). Pour cette étape, il est proposé de passer par le service smtp2go pour ceux qui souhaitent une solution simple à mettre en place ;
- vérification des droits en écriture ;
- mise en place d'un backup.

Et quelques étapes facultatives **[2]**.

Une fois ces étapes finalisées, vous pouvez lancer l'application :

```
elabctl start
```

La première connexion vous redirigera automatiquement vers la page **register.php** qui permettra de définir un compte administrateur. Les autres comptes pourront ensuite être créés depuis la même page.

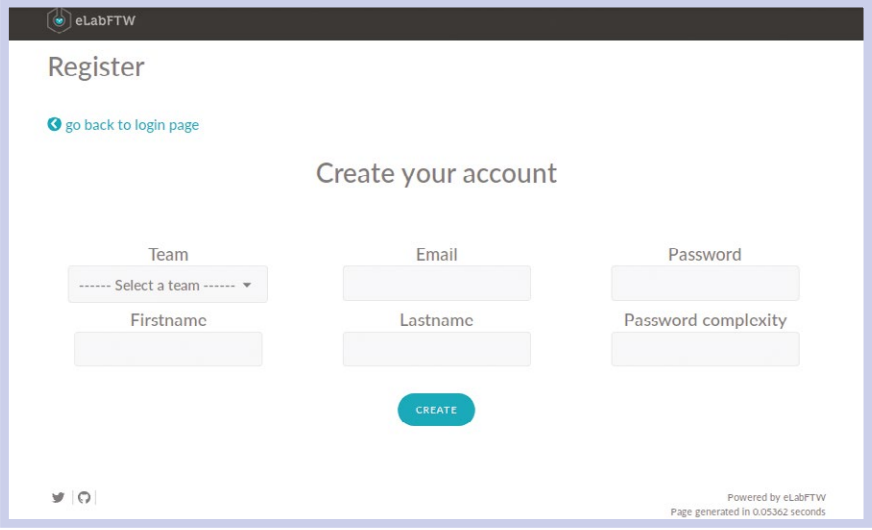


FIGURE 2. Une fois le compte administrateur créé, vous pourrez alors accéder aux différents paramètres d'eLabFTW, créer des comptes, etc.

3. MISE À JOUR

La mise à jour de l'application se fait assez simplement :

```
elabctl update
docker exec - it elabftw php bin/console db:update
```

Le temps de rédiger cet article, nous avons eu l'occasion de tester la mise à jour à plusieurs reprises (2.0.7 vers 3.0.1 puis 3.1), nous n'avons rencontré aucun problème.

Note : Si vous n'avez pas les compétences nécessaires, le temps ou l'envie d'installer et maintenir à jour votre propre serveur, l'auteur propose depuis peu un hébergement **[3]**.

4. UTILISATION

Une fois connecté, l'interface à laquelle vous faites face est relativement intuitive, le menu en haut (bandeau gris) comprend différentes entrées vous permettant d'accéder aux différentes fonctionnalités. Ce menu se présente sous la forme d'une icône « burger » si votre interface n'est pas très large puisque l'interface est adaptative. Détaillons ces entrées avant de voir le menu de l'utilisateur (en haut à droite) et le pied de page (tout ce qui concerne l'administration).

4.1 Expériences

Pressez [c] ou cliquez sur ***Créer > Expérience***, vous accèderez alors au formulaire de déclaration permettant de définir vos expériences, leurs buts, les procédures suivies, les résultats obtenus, définir des tags, etc.

Vous pouvez définir la visibilité de votre expérience pour la partager avec votre équipe, tout le monde ou la garder pour vous uniquement. Il est possible pour chaque expérience d'ajouter des commentaires.

Vous pouvez également joindre des fichiers ou faire un dessin rapidement à la main − du moins

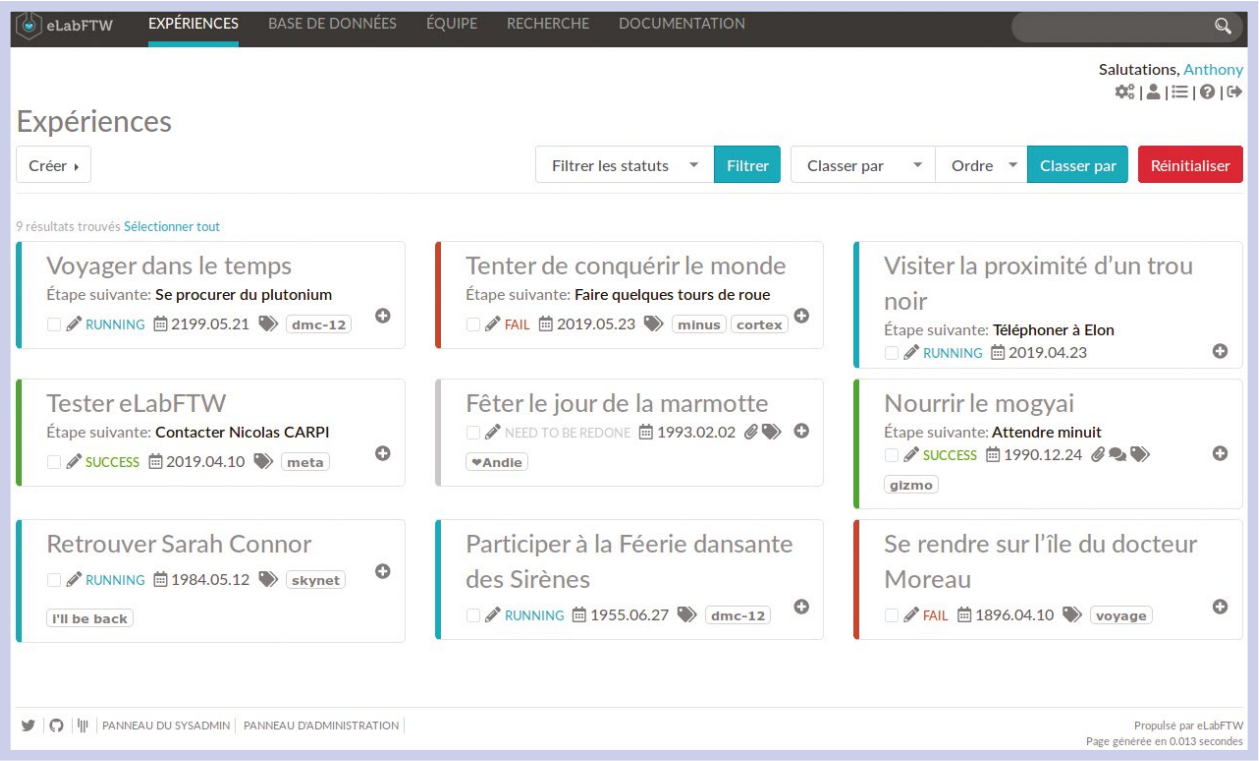


FIGURE 3. Pour l'instant, votre liste d'expériences est vide, mais voici ce à quoi elle ressemble une fois quelques entrées ajoutées.

à la tablette graphique, à la souris le résultat est rarement esthétique − idéal pour joindre directement un croquis d'expérience sans passer par un logiciel externe.

Chaque modification faite dans l'expérience est sauvegardée sous la forme d'une révision, vous pourrez donc revenir à une version précédente au besoin. Vous avez également la possibilité d'exporter vos données sous forme de ZIP ou de PDF.

Si vous avez l'habitude de présenter vos expériences toujours avec la même présentation, vous pouvez, si vous le souhaitez, définir un ou plusieurs modèles personnalisés qui vous permettront alors de gagner un temps certain lors de la création de celles-ci. Pour cela, rendez-vous dans ***Créer > Gérer les modèles***.

Une fois vos expériences créées, elles peuvent être triées selon leur statut et classées selon différents critères/tags (Figure 4, page suivante).

Une fois créées, vos différentes expériences sont listées sous forme de blocs dont la couleur varie en fonction de leur statut (cyan si elles sont en cours, vert pour les succès, gris pour les expériences nécessitant d'être refaites, rouge si elles ont échoué). En fonction de la taille de votre affichage, cette liste sera affichée en une, deux ou trois colonnes. Dans chaque bloc expérience sont affichés :

- une case à cocher pour sélectionner plusieurs expériences afin d'appliquer une modification ou exporter plusieurs entrées ;
- une icône crayon pour éditer le contenu ;
- le statut de l'expérience ;
- la date de création de l'entrée ;
- les tags que vous avez définis pour celle-ci, des icônes s'il y a des commentaires ou des fichiers joints ;
- un `+` permettant de développer le bloc.

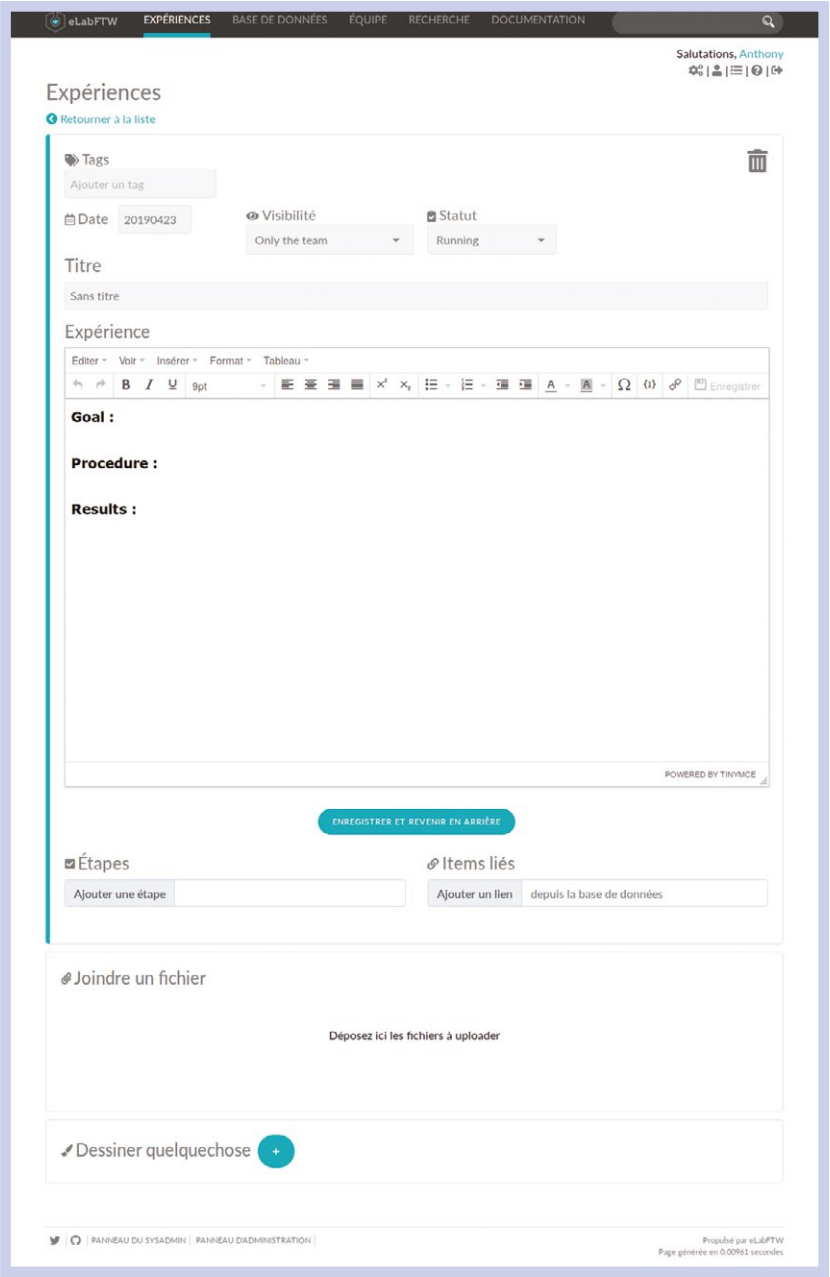


FIGURE 4. Création d'une expérience.

4.2 Base de données et équipe

L'entrée ***Base de données*** vous permet de définir un ensemble d'objets, éventuellement réservables (option à définir dans la catégorie). Ceci peut être particulièrement intéressant si certaines expériences nécessitent l'usage d'appareils spécifiques (formulaire ***Items liés*** dans le formulaire de création/modification d'expériences). La réservation de ces items se fait via le planificateur disponible dans le menu ***Équipe*** : il s'agit d'un calendrier de réservation permettant de définir les plages horaires d'utilisation des différents items.

Outre ce planificateur, le menu ***Équipe*** vous permet d'afficher la liste des membres de votre équipe, les modèles d'expériences de l'équipe, ainsi qu'un formulaire d'envoi de courriel.

4.3 Recherche

Un formulaire permettant d'effectuer une recherche selon différents critères dans l'ensemble de vos données est présent. Une fonction de recherche rapide est également disponible toute à droite de la page.

4.4 Documentation (et contribution)

On trouve un raccourci direct vers la documentation officielle **[4]**. Celle-ci est incroyablement complète, mais disponible uniquement en anglais.

Outre l'installation ou l'usage d'eLabFTW, vous trouverez également dans cette documentation, un ensemble d'informations à propos de la contribution **[5]**, n'hésitez pas à proposer votre aide, vos remarques, vos modifications, etc. Un coup de main est toujours le bienvenu ! Malgré le très faible nombre de contributeurs actuels, nous avons été témoins du dynamisme du développement d'eLabFTW : nous avons par exemple, dû procéder à plusieurs mises à jour durant la rédaction de cet article. De plus,

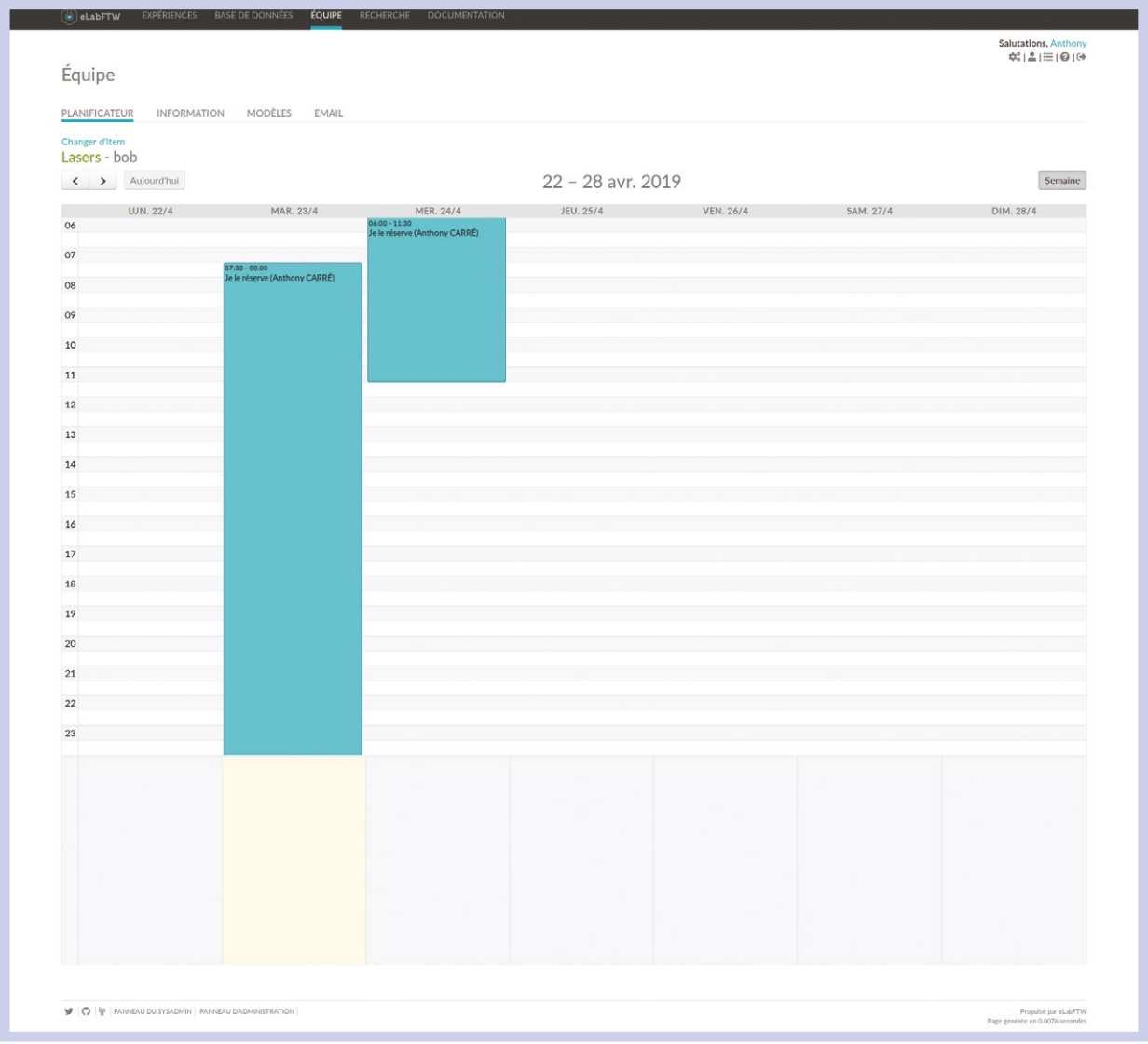


FIGURE 5. Réservez vos outils préférés pour éviter que vos collègues ne les empruntent.

nous avons profité de nos tests pour rapporter quelques bogues mineurs et faire des demandes de fonctionnalités, nous avons pu constater la réactivité impressionnante de l'auteur : nos demandes ont toutes été rapidement prises en charge et solutionnées, l'une d'entre elles ayant été résolue vingt minutes seulement après sa déclaration !

4.5 User-nav

Le menu de l'utilisateur se trouve à droite de la page, en dessous du menu principal (sur fond gris). Celui-ci se compose de cinq icônes :

- ***Paramètres*** : pour modifier vos préférences d'affichage, les raccourcis clavier, modifier votre mot de passe, vos informations de contact, créer et personnaliser vos modèles d'expériences. C'est également ici que vous pourrez sélectionner la langue de l'interface parmi pas moins de 13 langues, ce qui est très intéressant pour la plupart des laboratoires aujourd'hui !
- ***Profil*** : affichage d'informations et de statistiques ;

- ***Todoliste*** : une petite liste personnelle de choses à faire ;
- ***Aide*** : affichage d'une petite fenêtre d'aide ;
- ***Déconnexion***.

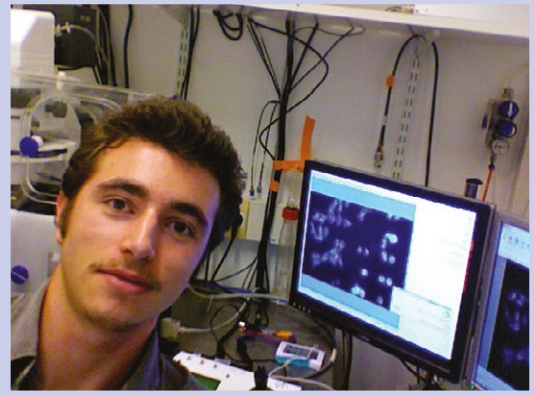
4.6 Panneau d'administration et panneau du sysadmin

Les liens vers ces pages de configuration sont disponibles en pied de page, la seconde uniquement pour les administrateurs, évidemment.

- Le panneau d'administration permet l'administration de l'équipe, des groupes, la recherche d'utilisateurs, la gestion des tags ou des modèles d'expériences…
- Le panneau du sysadmin permet l'affichage d'informations à propos de l'installation, des statistiques d'utilisation, les options de différents paramètres, etc. Tout le nécessaire de l'administrateur système.

CONCLUSION

ElabFTW est un outil intuitif, particulièrement intéressant, il peut remplacer avantageusement le cahier de laboratoire papier d'un chercheur. Un outil qui mériterait une plus grande renommée. N'hésitez pas à lui donner une chance, si vous êtes chercheur, essayez-le, vous ne le regretterez pas ! ■



Nicolas CARPI

4 QUESTIONS À NICOLAS CARPI, CRÉATEUR D'ELABFTW

1 Pouvez-vous vous présenter rapidement ?

Nicolas CARPI, ingénieur d'étude dans un laboratoire de recherche fondamentale en biologie cellulaire [6]. J'ai une formation de biochimiste et je fais de la biologie depuis une douzaine d'années. Et l'informatique et le Web prennent de plus en plus de place, car j'ai toujours aimé ça.

2 Vous êtes le développeur principal, pour ne pas dire unique [7]. C'est donc sur l'institut Curie et en particulier sur vous que repose la pérennité du logiciel…

En effet, les contributions au code par d'autres personnes sont minimes, et j'ai envie de dire « comme c'est souvent le cas dans le monde de l'open source ». Un exemple flagrant : GNUPG [8].

Néanmoins, je considère les gens qui ouvrent des issues sur GitHub comme des contributeurs, même s'ils ne produisent pas de code, ils aident à trouver les bugs ou proposent des améliorations, et ça a de la valeur à mes yeux. Et il ne faut pas oublier tous les gens qui ont permis de traduire eLabFTW dans 13 langues ! Ils n'apparaissent pas sur GitHub, mais leur travail est bien présent !

RÉFÉRENCES

Site officiel : https://www.elabftw.net

Démo : https://demo.elabftw.net

Code source : https://github.com/elabftw/elabftw

[1] Documentation installation : https://doc.elabftw.net/install.html

[2] Documentation post-installation : https://doc.elabftw.net/postinstall.html

[3] https://www.deltablot.com/elabftw

[4] Documentation : https://doc.elabftw.net/

[5] Contribuer : https://doc.elabftw.net/contributing.html

[6] https://science.curie.fr/recherche/physique-chimie-biologie-multi-echelle-et-cancer/umr144/equipe-piel/

[7] https://github.com/elabftw/elabftw/graphs/contributors

[8] https://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke

3 Il y a maintenant une double licence ? Pouvons-nous avoir confiance en l'avenir du projet libre ?

L'avantage d'un projet open source, c'est que si j'arrête de travailler dessus, je suis certain que d'autres prendront le relais. D'autre part, je pense qu'eLabFTW a atteint la taille critique, c'est-à-dire qu'il est désormais utilisé par suffisamment de labos à travers le monde pour qu'il y ait au moins un labo/université qui prenne le relais si jamais j'arrêtais de travailler dessus.

D'autre part, contrairement aux ELN hébergés par des entreprises, eLabFTW est « self-hosted », donc dans le pire des cas, si je disparais dans un trou noir, tout continuera de fonctionner parfaitement. Et les données sont facilement exportables dans de multiples formats.

Pour finir, j'ai créé une entreprise dans le but de vendre de l'hébergement eLabFTW (car tout le monde n'a pas le savoir-faire pour administrer un serveur) et aussi proposer le logiciel avec une licence commerciale (ce qui fait d'eLabFTW un projet à deux licences). Il y aura toujours la version libre et open source, mais aussi la possibilité d'acheter une licence commerciale pour les entreprises qui le souhaitent et qui sont allergiques à l'AGPL. Ce modèle est une des solutions pour permettre à un logiciel open source de survivre sur le long terme.

4 Quelles sont les grandes futures modifications que vous envisagez ?

Beaucoup d'utilisateurs souhaitent une plus grande flexibilité dans le choix des droits de visualisation/édition des expériences. C'est quelque chose que je n'avais pas imaginé au début du logiciel. Car si on compare avec un cahier de laboratoire papier, ça me ferait bizarre que quelqu'un d'autre que moi écrive dedans. Pourtant, beaucoup de gens souhaitent ce genre de *feature*, qui est déjà accessible, mais pas suffisamment flexible. Je vais donc m'atteler à cette tâche.

LE RGPD EXPLIQUÉ

aux informaticiens

OLIVIER AUVERLOT

ENTRÉ EN APPLICATION LE 25 MAI 2018, LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES EST UNE AVANCÉE MAJEURE POUR LA PROTECTION DES DONNÉES PERSONNELLES. IL EST POURTANT SOUVENT PERÇU DE DIFFÉRENTES FAÇONS. CERTAINS LE CRAIGNENT DE MANIÈRE EXAGÉRÉE ALORS QUE D'AUTRES LE NÉGLIGENT OU MÊME L'IGNORENT TOTALEMENT. IL EST DONC TEMPS DE FAIRE LE POINT SUR CE TEXTE ET SUR CE QU'IL IMPLIQUE CONCRÈTEMENT POUR LES INFORMATICIENS.

Le problème de la protection des données personnelles n'est pas nouveau. Au début des années 70, le projet SAFARI vise à interconnecter des fichiers nominatifs de l'administration française. Révélé au grand public par un article de presse, ce projet déclenche un débat sur la protection de la vie privée et surtout donne naissance à la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mais aussi à une autorité indépendante bien connue sous le nom de CNIL (Commission Nationale de l'Informatique et des Libertés). En 1995, l'Union Européenne adopte la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

L'informatique évolue sans cesse et les lois doivent s'adapter. Depuis le début des années 2000, la problématique de la protection des données personnelles est devenue de plus en plus importante et complexe. Ces années sont celles de l'Internet grand public et surtout des services dans les nuages (*cloud computing*) auxquels de plus en plus de particuliers et d'entreprises confient des données personnelles. De nombreuses affaires ont fait la une de l'actualité telles que les révélations d'Edward Snowden en 2013 **[1]** ou encore le scandale Facebook-Cambridge Analytica à partir de 2016. L'arrivée dans nos foyers de l'Internet des objets (IoT) pose également de nombreuses questions sur la justification de la captation de certaines données à l'insu des personnes. En février 2019, Nest, filiale de Google, révèle la présence d'un micro dans la base Nest Guard de son système d'alarme Nest Secure **[2]**. En avril 2019, Bloomberg découvre que l'assistant électronique Alexia enregistre, via l'enceinte connectée Amazon Echo **[3]**, des millions de conversations qui sont ensuite écoutées par des salariés de l'entreprise. Smartphone, montre, thermostat, voiture… notre vie quotidienne est maintenant remplie d'objets connectés qui collectent sans cesse des données sur notre activité quotidienne et nos centres d'intérêt. Ces données s'échangent, se vendent pour quelques dollars ou sont même volées pour être revendues sur le Darknet.

Pour protéger les personnes physiques de la divulgation ou d'une exploitation sans limites de ces données, la Commission Européenne a voté et adapté le RGPD en 2016. Ce texte a été adopté à la France par la loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Son objectif est la protection de la vie privée des personnes et des libertés publiques par l'affirmation que les personnes fichées ont des droits et qu'il faut respecter un cadre strict pour l'utilisation de données personnelles. Nous sommes tous concernés par cette loi en tant que citoyens. Il s'agit d'apprendre à protéger ses données personnelles et à respecter celles des autres.

1. TRAITEMENT ET DONNÉES

Les notions de traitement et de données personnelles sont au centre du RGPD. Il est impossible de l'appliquer si vous ne connaissez pas la définition exacte de ces termes. Le vocabulaire a donc ici une grande importance.

1.1 Définition d'un traitement

Le traitement de données à caractère personnel fait référence à toute opération ou tout ensemble d'opérations appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. Il est important de savoir que ces opérations peuvent être effectuées ou non à l'aide de procédés automatisés. Cela signifie donc que limiter l'application du RGPD au seul domaine des traitements informatisés est une erreur. Des données personnelles stockées sur du papier ou des enregistrements (vidéo ou sonores) sont également concernées par le RGPD. Mettre en application le RGPD ne consiste pas à se pencher uniquement sur les traitements informatiques d'une organisation, mais sur l'ensemble de ses procédures techniques et administratives.

1.2 Données personnelles et données sensibles

Une donnée personnelle est une information ou une combinaison d'informations permettant d'identifier directement ou indirectement une personne physique. Ce terme désigne donc un large spectre de types de données et ne se limite pas aux seuls noms, prénoms et dates de naissance. On peut en effet prendre en compte un numéro de téléphone, une adresse de courrier électronique, un identifiant de badge d'accès, ou encore des informations de géolocalisation. Sachez également que l'adresse IP collectée est considérée comme étant une donnée personnelle.

Le RGPD définit également les données dites sensibles dont la collecte et le traitement imposent des mesures spécifiques. Il s'agit des origines raciales ou ethniques, des opinions politiques, des convictions religieuses ou philosophiques, de l'appartenance syndicale, des données biométriques (photographie, empreinte digitale, etc.), des données de santé et de celles portant sur la vie sexuelle ou l'orientation sexuelle. Pour ces données sensibles, il est souvent nécessaire de demander l'avis à la CNIL et de faire une analyse d'impact (AIPD). Cette étude doit être réalisée pour les traitements présentant un risque élevé. Si votre traitement correspond à deux des critères suivants, vous êtes dans l'obligation de la réaliser :

- évaluation/notation ;
- décision automatisée avec effet judiciaire ou effet similaire ;
- surveillance automatisée ;
- données sensibles ou hautement personnelles ;
- données personnelles traitées à grande échelle ;
- croisement de données ;
- données portant sur des personnes vulnérables ;
- usage innovant ;
- exclusion du bénéfice d'un droit, d'un service ou d'un contrat ;

Pour aider le responsable de traitement, la CNIL met gratuitement à disposition un logiciel informatique nommé PIA **[4]** disponible sous la forme d'une application installable directement sur un micro-ordinateur ou sur un serveur pour un accès web.

La collecte des données à caractère personnel est fortement encadrée par le RGPD. Celle-ci doit être loyale : les données ne peuvent être collectées à l'insu des individus. Le traitement doit être explicite, déterminé et également justifié par des finalités légitimes reposant sur une ou plusieurs bases légales. La finalité du traitement doit être respectée par le responsable de traitement durant toute la durée du traitement et ne pas être détournée. De plus, un individu doit consentir librement à une collecte de données personnelles. Son consentement doit être spécifique au traitement et il doit être éclairé, ce qui signifie qu'il doit être préalablement informé de la nature et de l'usage qui sera fait de ses données. Il peut d'ailleurs être important de tenir un registre des consentements, de conserver la preuve qu'une personne a accepté que ses données à caractère personnel soient utilisées dans un traitement. La collecte de données personnelles doit également être proportionnée, seules

LES BASES LÉGALES DU RGPD

Le RGPD spécifie six bases légales possibles pour définir un traitement :

- **consentement préalable de la personne concernée ;**
- **exécution d'un contrat ;**
- **obligation légale ;**
- **sauvegarde des intérêts vitaux de la personne ;**
- **mission de service d'intérêt public ou relevant de l'exercice de l'autorité publique ;**
- **intérêt légitime du responsable de traitement ou d'un tiers.**

les données indispensables au traitement doivent être demandées. Ce principe de minimisation est un élément clé du RGPD. Avez-vous vraiment besoin de la date de naissance de la personne ? Est-ce que l'âge ne suffit pas par exemple ? Réduire la quantité de données personnelles facilite grandement l'anonymisation ou la pseudonymisation (séparation des données à l'aide de deux fichiers non connectés et dont les enregistrements sont joints à l'aide d'une clé) au sein de bases de données, mais cela ne résout pas tous les problèmes liés à ces deux opérations. Parfois en effet, des informations qui en soi ne disent rien de particulier sur une personne peuvent constituer des données personnelles en étant associées les unes aux autres. Il est ainsi aisé par déduction de déterminer l'identité d'un individu. Constituer un fichier anonymisé n'est donc pas si simple qu'il n'y paraît.

1.3 Une attribution claire des rôles

Le RGPD définit avec précision les rôles des différents acteurs de la mise en conformité. Il s'agit principalement du responsable du traitement et du délégué à la protection des données (DPD). En complément, d'autres acteurs historiques restent impliqués dans la protection des données personnelles. Les responsables des services informatiques, les directions juridiques ou les responsables de la Sécurité des Systèmes d'Information (RSSI) doivent travailler de manière transversale avec le responsable du traitement et le Délégué à la Protection des Données. Autre grosse nouveauté du RGPD, la notion de sous-traitant est également prise en compte.

1.3.1 Le responsable du traitement

Le responsable du traitement détermine les finalités et les moyens du traitement. Il doit mettre en œuvre des mesures techniques et organisationnelles pour assurer la confidentialité des données personnelles. Il doit être capable de démontrer que le traitement est assuré conformément au RGPD. Enfin, il doit faire appliquer des mesures appropriées en matière de protection des données. Le responsable du traitement engage sa responsabilité pénale et cette responsabilité peut être partagée avec d'autres personnes.

Il est au sommet de la hiérarchie de l'organisation et il est le responsable légal de l'application du RGPD. En fonction du statut de l'organisation, il peut s'agir du chef d'entreprise, du recteur d'une Académie, du Président d'une Université ou encore du Président d'une association (loi de 1901).

1.3.2 Le délégué à la protection des données

Le DPD ou DPO (*Data Protection Officer*) remplace le CIL (Correspondant Informatique et Libertés), mais n'est pas forcément un ancien CIL. Il est obligatoire pour les autorités ou les organismes publics, les entreprises dont les activités de base sont de réaliser un suivi régulier et systématique des personnes à grande échelle et les organismes traitant des données dites « sensibles ». Le DPD informe et conseille le responsable du traitement, les sous-traitants et le personnel. Il coopère avec l'autorité de contrôle (la CNIL en France). Il assure la bonne tenue de la documentation relative au traitement. Il a également un rôle de conseil et de validation pour la mise en œuvre d'une analyse d'impact.

Le **droit d'opposition** permet à une personne de refuser que ses données soient exploitées par un traitement. Ce droit ne peut pas être systématiquement appliqué en fonction de la raison d'être du traitement (une obligation légale par exemple). Dans tous les cas, ce droit n'est pas un droit à la suppression de toutes les données ou du compte qui est rattaché à une personne.

Pour demander la suppression de données à caractère personnel la concernant, une personne doit faire usage de son **droit à l'effacement**. L'usage de celui-ci n'est possible que pour l'une des six situations suivantes :

- les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
- la personne retire son consentement au traitement des données ;
- la personne s'oppose au traitement et il n'existe pas de motif légitime impérieux ;
- le traitement est illicite ;
- les données doivent être effacées pour respecter une obligation légale ;
- les données ont été collectées auprès de mineurs.

Ce droit à l'oubli est complété par le droit de suite qui impose à l'organisation ayant traité la demande d'effacement de communiquer cette demande à ses éventuels sous-traitants. Le respect de ce droit impose donc un suivi des demandes et une cartographie à jour des flux de données.

Le **droit à la portabilité** permet à une personne de récupérer les données personnelles qu'elle a fournies à une organisation. Ce droit n'est applicable que si le traitement est effectué à l'aide de procédés automatisés et s'il est fondé sur le consentement de la personne ou sur un contrat. Le RGPD n'impose aucun format de fichier spécifique pour cette opération, mais recommande un format ouvert et lisible par un logiciel. Ce droit inclut également la possibilité de transmettre les données à un nouveau responsable de traitement.

Le **droit à la limitation** du traitement est destiné à geler l'utilisation de données à caractère personnel détenues par une organisation afin de permettre à une personne physique d'appliquer ses droits d'opposition et de rectification. L'organisme ne peut que conserver les données et aucune exploitation n'est possible. Ce droit permet également à une personne d'empêcher l'effacement de ses données personnelles alors que l'organisation qui les détient veut les supprimer.

Enfin, le RGPD définit le **droit de ne pas faire l'objet d'une décision exclusivement fondée sur un traitement automatisé** et plus particulièrement si celle-ci a un effet juridique ou l'affecte sensiblement. Le recours à ce droit est rendu caduc si la personne concernée a donné son consentement explicite, si la décision est nécessaire dans le cadre d'un contrat ou si la décision automatisée est autorisée par des dispositions légales spécifiques. Mais dans tous les cas, l'organisme doit prévenir la personne concernée qu'une décision automatisée a été prise, qu'elle a le droit de la contester et qu'elle peut demander un nouvel examen de la décision par un être humain.

1.5 Prise en compte des flux de données

Étant donné que nous vivons dans l'ère de la mondialisation numérique et que les données circulent de pays en pays via les « autoroutes de l'information », il est nécessaire que le RGPD crée une bulle de protection autour des données personnelles. Le RGPD protège ainsi les citoyens européens, quel que soit l'endroit où sont stockées leurs données (dans l'Union Européenne ou non). De même, le RGPD protège les données personnelles des citoyens non européens à partir du moment où celles-ci sont hébergées par des services situés dans la Communauté Européenne.

Lorsque les données transitent dans et hors de l'Union Européenne **[5]**, le niveau de protection doit rester équivalent et les principes du RGPD doivent être respectés par l'ensemble des destinataires successifs. Si le pays n'est pas considéré comme étant adéquat, les transferts sont réalisés sous des conditions strictes (règles d'entreprise contraignantes, certifications, codes de conduites, clauses contractuelles) **[6]**. Dans certains cas, il faut obtenir une autorisation de transfert de la part de

l'autorité de protection des données. Dans quelques cas, il faut pouvoir se prévaloir de l'une des dérogations énumérées par l'article 49 du RGPD concernant les dérogations pour des situations particulières.

2. LE PRINCIPE D'ACCOUNTABILITY

Pour le responsable de traitement, il s'agit de l'obligation de mettre en œuvre et de documenter des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. Le responsable de traitement doit fixer un cadre de collecte et d'utilisation des données à caractère personnel conforme au RGPD et doit le respecter. Ce principe met fin à celui de la déclaration des traitements auprès de la CNIL. Le responsable de traitement, conseillé par son DPD, doit mettre en œuvre les différents outils de mise en conformité. Il reste cependant quelques cas particuliers où cette déclaration est nécessaire tels qu'une demande d'avis (utilisation de données sensibles, transferts de données hors Union Européenne, etc.), une étude génétique de populations, la description d'un dispositif technique, le contrôle de l'activité des salariés, une demande d'autorisation dans le domaine de la santé ou encore une collecte d'échantillons de substances corporelles humaines.

2.1 Cartographie des traitements

Pour mettre en œuvre le RGPD, une organisation doit être capable d'établir une cartographie des traitements qu'elle exploite. Ce document regroupe des traitements automatisés, mais également des traitements réalisés par des êtres humains (procédures administratives par exemple). Elle doit référencer les informations essentielles telles que le nom du traitement, sa finalité, les interlocuteurs, les catégories de données traitées, les données à risques, les destinataires des données, les flux et transferts de données, les sous-traitants, l'hébergement des données ou encore l'application d'une politique d'archivage.

Ce tableau est sommaire, mais il constitue une synthèse permettant de détecter les traitements à risques (manipulation de données à caractère personnel). Pour chacun d'entre eux, il faudra compléter une fiche de registre et constituer ainsi votre registre des traitements.

2.2 Le registre des traitements

Ce registre est l'élément essentiel d'une organisation pour prouver sa conformité au RGPD. Il rassemble l'ensemble des fiches de registre décrivant les traitements de données à caractère personnel. Pour aider le responsable de traitement, la CNIL publie sur son site web un modèle de fiche contenant les informations essentielles **[7]**. Le responsable de traitement est libre d'enrichir ce modèle en fonction de ses besoins. Si on se réfère au RGPD et aux différentes publications énumérant les bonnes pratiques, on peut décomposer une fiche de traitement en cinq grandes parties.

2.2.1 Informations générales sur le traitement

En premier lieu, il est important de décrire le traitement à l'aide d'un certain nombre d'informations générales telles que le nom et la description du traitement, la date d'ouverture du dossier, les dates de début et de fin du traitement, les noms et les coordonnées du responsable de traitement, du délégué à la protection des données ainsi que celles du responsable des services opérationnels traitant les données.

2.2.2 Les données personnelles traitées

Il est temps maintenant de s'occuper des données personnelles en précisant tout d'abord les

Pour pouvoir travailler efficacement, le DPD doit être indépendant, ne pas subir de pressions et être protégé de tout conflit d'intérêt. La fonction de DPD n'est donc pas compatible avec celle de DSI, de RSSI ou de directeur juridique. Il peut être un juriste avec de bonnes notions techniques et plus particulièrement en sécurité informatique ou un informaticien ayant une connaissance approfondie de la règlementation. Par ailleurs, il doit posséder une bonne connaissance des rouages de l'entreprise, de son organisation et de son fonctionnement.

1.3.3 Le sous-traitant

Dans le domaine du traitement des données personnelles, les obligations d'un sous-traitant sont très accentuées. Il n'agit qu'à la demande du responsable du traitement de son client. Le sous-traitant est responsabilisé et doit pouvoir jouer un rôle de conseil auprès du responsable de traitement. Il doit faire preuve de transparence, mettre en œuvre une traçabilité sur les données et les traitements associés. Ceux-ci sont obligatoirement mis en œuvre dans un environnement sécurisé.

Un responsable de traitement doit donc choisir un sous-traitant présentant des garanties suffisantes au regard du RGPD. Ces garanties sont formalisées dans un accord à l'aide de clauses contractuelles spécifiques.

1.3.4 La nouvelle CNIL

Avec le RGPD, les missions de la CNIL ont évolué. Elle doit informer et conseiller les organisations et le grand public pour la mise en œuvre du RGPD et pour défendre les droits des citoyens. Elle a également une mission de veille et de prospective sur les nouveaux usages des outils informatiques. Elle doit réfléchir sur les problèmes éthiques tels que ceux liés à la biométrie ou aux données génétiques.

Dans certains cas, elle doit encore être consultée et conserve un pouvoir d'autorisation. Elle a enfin un pouvoir d'enquête, mais aussi de répression. La CNIL a précisé dans un communiqué daté du 19 avril 2019 que « *Désormais, la CNIL vérifiera pleinement le respect des nouvelles obligations et nouveaux droits issus du cadre européen (analyse d'impact, portabilité des données, tenue d'un registre des traitements et des violations) et tirera, au besoin, toutes les conséquences en cas de constatation de manquements* ». Les sanctions ont été considérablement renforcées dans le cadre du RGPD et les peines peuvent aller jusqu'à :

- des sanctions pécuniaires à hauteur de 20 millions d'euros ou de 4% du chiffre d'affaires mondial d'une entreprise ;
- 300 000 euros pour une personne physique ;
- 1,5 million d'euros pour une personne morale ;
- jusqu'à 5 ans de prison.

À cela, il faut également ajouter une détérioration de l'image de marque et une très mauvaise publicité pour une entreprise ou une administration. Faire les gros titres de la presse pour non-respect du RGPD n'est vraiment pas un gage de confiance.

1.4 Affirmation des droits des personnes

L'affirmation des droits des personnes est primordiale au sein du RGPD. Les personnes physiques doivent avoir le contrôle des données à caractère personnel les concernant et surtout avoir connaissance des détails de l'utilisation de leurs données.

Le **droit à l'information** oblige une organisation mettant en œuvre un traitement de données personnelles à informer les personnes fichées de son identité, de l'objectif de la collecte d'informations, de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne et des transferts de données vers un pays ne faisant pas partie de l'Union Européenne.

Avec le **droit d'accès**, une personne peut vérifier qu'elle est toujours présente dans un fichier, prendre connaissance des données personnelles détenues par une organisation et vérifier leur exactitude. Si ce n'est pas le cas, une personne physique peut utiliser son **droit à la rectification** afin de corriger les informations inexactes et compléter des données en lien avec la finalité du traitement.

catégories auxquelles elles appartiennent (identité, données bancaires, etc.), la méthode de leur collecte et les données identifiant directement ou indirectement une personne. Si des données sensibles sont traitées et donc susceptibles de soulever des risques en raison de leur sensibilité particulière, il est nécessaire de préciser la nature du risque, de documenter la réalisation d'une analyse d'impact et éventuellement fournir la référence d'une déclaration spécifique à la CNIL.

Dans tous les cas, vous devez préciser si les données sont sujettes à une interconnexion de fichiers, les lieux où les données sont hébergées ainsi que la durée de conservation de celles-ci. La fiche de traitement doit également préciser les catégories de personnes concernées par le traitement et les modalités d'information auprès des usagers.

2.2.3 Finalités et fondement juridique

L'étape suivante consiste à fournir les raisons pour lesquelles les données ont été collectées. Il s'agit ici d'expliquer l'utilité de chaque donnée et de démontrer qu'elle est indispensable pour la réussite du traitement. Ce dernier doit également reposer sur un fondement juridique qui peut être le consentement de la personne concernée, l'exécution d'un contrat, une obligation légale, la sauvegarde des intérêts vitaux de la personne concernée, une mission de service d'intérêt public, l'intérêt légitime du responsable de traitement ou d'un tiers et enfin l'intérêt général (recherches historiques ou scientifiques par exemple).

2.2.4 Acteurs du traitement

Il est maintenant important de documenter les acteurs du traitement, c'est-à-dire ceux qui accèderont à l'intégralité ou à une sous-partie des données à caractère personnel collectées. Ces acteurs peuvent être internes ou externes à votre organisation. Si des sous-traitants sont impliqués dans le traitement des données personnelles, ils doivent être référencés dans la fiche de traitement et les catégories de données qui leur sont confiées doivent être indiquées. Si nécessaire, vous devez également indiquer vers quels pays les données sont transférées. Dans le cas d'un transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission Européenne et sans certaines garanties précises (articles 46 et 47 du RGPD), des garanties spécifiques devront être prévues et documentées.

Enfin, n'oubliez pas de préciser si une procédure d'habilitation des personnels a été mise en place pour l'accès aux données et précisez le type de cette habilitation.

2.2.5 Les mesures de protection des données

En complément des mesures prises globalement pour protéger les données du système d'information, il est également nécessaire de documenter les mesures mises en œuvre spécifiquement pour le traitement des données à caractère personnel. Vous devez ici prouver que tout est fait, tant sur le plan technique qu'organisationnel, pour protéger les informations. Il convient ici d'insister sur les droits d'accès aux données accordés aux utilisateurs, sur le contrôle des sous-traitants, sur les méthodes d'anonymisation ou de pseudonymisation des données, sur la sécurisation des flux de données ou encore sur les mesures de traçabilité des opérations.

2.3 Communication du registre

Le registre doit pouvoir être communiqué à la CNIL lorsqu'elle le demande. Les organismes du secteur public sont tenus de transmettre le registre à toute personne qui en fait la demande, car il s'agit d'un document administratif, communicable à tous, au sens du code des relations entre le public et les

administrations. Bien évidemment, il peut être nécessaire d'avoir retiré préalablement toutes les informations dont la divulgation pourrait porter atteinte à des données confidentielles ou compromettre la sécurité des systèmes d'information.

2.4 Compléter son registre des traitements

Afin de renforcer sa mise en conformité, il est souhaitable de mettre en œuvre d'autres outils destinés à compléter les fiches descriptives des traitements et enrichir ainsi le registre de l'organisation.

2.4.1 Registre des consentements

Si les traitements mis en œuvre par votre organisation nécessitent le consentement préalable de l'utilisateur, il est recommandé de mettre en œuvre un registre des consentements. Celui-ci doit conserver une trace de ce consentement afin que le responsable du traitement soit en mesure de démontrer que la personne a bien consenti, dans des conditions valides.

2.4.2 Notification des violations de données

Le registre des failles de sécurité référence les failles pouvant engendrer un risque pour les droits et libertés des personnes concernées. Pour chaque faille détectée, il faut indiquer sa date de découverte, le type d'atteinte, l'importance de l'atteinte aux données personnelles, les mesures prises pour y remédier et les mesures prises pour que ce risque ne se réitère pas. Une violation de sécurité doit être obligatoirement notifiée à la CNIL dans les 72 heures. Par contre, le responsable du traitement n'a l'obligation de prévenir les utilisateurs concernés que lorsque la violation de leurs données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

2.4.3 Documenter la sécurité et l'organisation du système d'information

Le registre des traitements doit être complété par des références aux documents décrivant les mesures organisationnelles ainsi que la sécurisation logique et physique du système d'information de l'organisation. Encore une fois, le responsable de traitement doit être capable de démontrer que toutes les mesures nécessaires ont été prises pour garantir la sécurité des données à caractère personnel.

Ces documents, le plus souvent supervisés par le RSSI de l'organisation, décrivent la sécurisation des postes de travail (authentification, antivirus, chiffrement du stockage, etc.), des serveurs (authentification, mises à jour, sauvegardes, etc.) et de l'infrastructure réseau. Ils présentent les mesures prises pour la sécurisation des locaux (contrôle d'accès, surveillance, gestion des pannes électriques ou des incendies, etc.). Ils exposent les mesures de traçabilité (journaux systèmes, etc.). Cette documentation est généralement complétée par un PRA (Plan de Reprise d'Activité) donnant la marche à suivre en cas d'incident grave.

3. PRIVACY BY DESIGN

Le RGPD impacte fortement le développement et le déploiement d'applications traitant des données à caractère personnel. Dès la phase de conception d'un traitement, il est fondamental de mettre en œuvre une approche visant à garantir la protection de la vie privée. Pour cela, le RGPD met en avant le concept de *Privacy by Design* permettant d'offrir le plus haut niveau possible de protection des données à caractère personnel.

3.1 Sécuriser les traitements

Dans le cadre de la collecte et de la manipulation de données à caractère personnel, il est indispensable de sécuriser les traitements concernés. L'objectif est de garantir l'intégrité, la confidentialité et la disponibilité des données. Les mesures prises doivent

être adaptées à la nature des données et aux risques présentés par le traitement. Elles concernent la sécurisation physique des données (gestion des accès à la salle des serveurs, système de lutte anti-incendie, protection contre les coupures électriques, sécurisation des postes clients, etc.). Serveurs et postes clients doivent être sécurisés (mises à jour du système d'exploitation et des logiciels, solution antivirus, etc.). Il est important de sensibiliser le personnel sur le respect des données personnelles, d'éviter l'utilisation de moyens de stockage amovibles (disques durs externes, clés USB, etc.), de mettre en place une gestion des postes mobiles (ordinateurs, smartphones, tablettes, etc.). Le chiffrement des données sur les postes clients est un bon moyen de limiter les risques liés au vol ou à la perte d'une machine.

Au niveau de la sécurité logique, l'architecture réseau doit mettre en œuvre une segmentation afin de contrôler les flux de données. Les protocoles réseau utilisés doivent être sécurisés à l'aide de méthodes de chiffrement. Dans le domaine des applications web, il est requis d'utiliser le protocole HTTPS pour assurer les échanges de données entre le poste client et le serveur. L'accès aux données dans les applications doit être géré à l'aide d'un mécanisme d'authentification basé sur des mots de passe robustes et une gestion des droits des utilisateurs afin de garantir que les informations ne sont accessibles qu'aux personnes autorisées.

Vous trouverez sur le site de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) un ensemble de documents regroupant les bonnes pratiques essentielles pour sécuriser une infrastructure de services **[8]**.

Sur le plan organisationnel, le RGPD renforce l'importance de la réalisation d'une cartographie des traitements. Celle-ci permet à une organisation de recenser l'ensemble des traitements existants et de détecter ainsi ceux comportant des données à caractère personnel. Pour une DSI, c'est une opportunité pour lutter contre le *shadow IT* : des traitements mis en œuvre par les membres de l'organisation, mais inconnus du service informatique et donc hors de son contrôle. Une fois évalués en terme de fonctionnalités et de risques, ces traitements clandestins pourront être remplacés par des outils respectant les règles de l'organisme.

Il faut également noter le rôle important du DPD en ce qui concerne la réévaluation continue de la protection des données. Les outils de la mise en conformité doivent être régulièrement mis à jour pour prendre en compte l'évolution du système d'information. Des évaluations telles que des tests d'intrusion ou des essais de restauration de données doivent être menées périodiquement. Ces différentes actions imposent l'établissement de relations étroites entre les différents acteurs impliqués (DPD, RSSI, responsables du déploiement, administrateurs système et développeurs) ainsi que la sensibilisation et la formation du personnel de l'organisme. La politique de sécurité d'un système d'information doit être complétée par une charte d'utilisation présentant aux collaborateurs leurs droits et devoirs en matière de sécurité. Elle est également l'occasion de préciser le périmètre d'utilisation autorisé par l'organisme en ce qui concerne les applications autres que celles déployées par la DSI (applications cloud en particulier).

3.2 Encadrer la saisie de données

Les formulaires de saisie sont les principaux éléments d'interface exploités par les utilisateurs. Dans le cadre d'applications telles que celles concernant les ressources humaines, leurs champs de saisie reflètent généralement une grande part des données collectées et traitées. Sur un site web, un formulaire de contact ou une procédure d'inscription, sont également des éléments d'interface susceptibles de collecter des données à caractère personnel. Pour respecter le RGPD, il est donc nécessaire de les concevoir avec attention.

En premier lieu, un formulaire doit limiter la saisie des données personnelles au strict minimum. Une information qui n'est pas indispensable au traitement ne doit pas être demandée à l'utilisateur. De plus, il ne faut pas rendre obligatoire systématiquement l'intégralité des champs de saisie. Si la collecte d'une information ne

rend pas impossible la réussite du traitement et que celui-ci peut atteindre ainsi son but, l'utilisateur doit avoir la possibilité de ne pas la saisir. Cette minimisation de la saisie pousse également à éviter l'usage des champs de saisie libres tels que la balise HTML `<textarea>`. Ces zones fourre-tout servent généralement à apporter un commentaire ou un complément aux autres données saisies. Le problème est qu'il est difficile de cadrer l'utilisation réelle de ce type de champ par les utilisateurs de l'application. Comment les empêcher de saisir des données à caractère personnel et même sensible alors qu'il n'y a aucun besoin de le faire ? En supplément d'une sensibilisation des utilisateurs au RGPD, il convient d'avoir recours à un maximum de champs limitant la collecte de données à celles prédéfinies au sein de nomenclatures. L'exploitation des données en sera facilitée et vous ne prendrez pas le risque d'être hors-la-loi.

Le second point important avec les formulaires est celui de la transparence avec l'utilisateur. Dans le cadre du RGPD, le consentement à un traitement doit être libre, spécifique, éclairé et univoque. C'est pourquoi il ne faut pas tenter de forcer la main de l'utilisateur en fixant par défaut la valeur de certains champs (des cases à cocher par exemple) pour que la personne s'inscrive involontairement à un abonnement, à un service commercial ou encore pour rendre publiques des données personnelles. De même, les options de configuration par défaut doivent obligatoirement être celles qui protègent les données personnelles (*Privacy by Default*). Il est crucial que l'utilisateur comprenne le traitement appliqué à ses données, qu'il puisse choisir sans contrainte d'accepter ou de refuser le traitement et qu'il puisse changer d'avis librement. Pour atteindre ces objectifs, il faut mettre en œuvre tous les moyens possibles pour expliquer à la personne concernée la raison de la collecte d'une donnée personnelle et l'usage qui en sera fait. Dans un formulaire, vous devez indiquer clairement les champs devant être obligatoirement complétés. Vous pouvez utiliser des bulles d'aide contextuelles afin d'informer l'utilisateur sur la raison de la collecte de la donnée et préciser le périmètre de sa diffusion. Vous devez obligatoirement insérer une information concise, transparente, compréhensible et aisément accessible aux personnes concernées **[9]**. Celle-ci indique l'identité du responsable du traitement, la finalité du traitement, le caractère obligatoire ou facultatif des données collectées et l'existence de droits des personnes concernées.

Un formulaire de collecte de données à caractère personnel doit également disposer d'un moyen clairement identifié et simple d'utilisation afin de recueillir le consentement de l'utilisateur. L'entrée et la sortie volontaire d'un traitement sont parfaitement illustrées par les mécanismes dénommés *Opt-in* et *Opt-out*. Ces termes issus du marketing, concernent l'usage d'adresses de courrier électronique dans le cadre de la prospection commerciale. Le consentement devant être libre, spécifique et éclairé, il doit être possible à tout moment de le retirer. Puisque la notion prévue par les textes est celle de l'accord entre les deux parties, une information préalable de la personne est nécessaire, accompagnée d'un moyen pour celle-ci de signifier sans équivoque son accord. La CNIL (décembre 2013) recommande une mention d'information donnant accès à une page plus détaillée précisant la finalité, le moyen de s'opposer à la poursuite du traitement et parfois également au traçage.

» ATTENTION

Les listes de diffusion

Dans le cadre d'une liste de diffusion, il est possible d'enregistrer l'adresse de courrier électronique d'une personne et de ne pas autoriser sa sortie de la liste. Cela est autorisé uniquement si la liste fournit des informations importantes et indispensables au bon fonctionnement de l'entreprise ou de l'administration.

3.3 Ne pas dissimuler les mécanismes de traçage et de collecte

La transparence de la collecte et du traitement de données à caractère personnel passe par l'information des personnes. Il n'est donc pas acceptable de

Bienvenue !
La présente section vous permet de personnaliser vos choix quant à la collecte et au traitement des données que nous et nos partenaires sommes amenés à effectuer.
Pour en savoir plus sur les cookies, sur les données que nous utilisons, sur vos droits concernant ces traitements et les partenaires avec qui nous travaillons, vous pouvez consulter notre politique d'usage des cookies.
VOUS AUTORISEZ
+ Conservation et accès aux informations
+ Évaluation
+ Personnalisation
+ Sélection, diffusion et signalement de contenu
+ Sélection, diffusion et signalement de publicités
Refuser
Accepter
PAR TOUS NOS PARTENAIRES
Voir nos partenaires
PRIVACY MANAGEMENT BY DIDOMI
Refuser tout
Accepter tout

FIGURE 1. Exemple de paramétrage de traceurs sur un site web.

mettre en œuvre des mécanismes cachés œuvrant à la collecte de données personnelles à l'insu de la personne. Sur le web, cette collecte est souvent basée sur le traçage des utilisateurs afin d'étudier leurs comportements sociaux, leurs déplacements ou encore leurs habitudes de consommation. Des mentions légales doivent obligatoirement communiquer les informations essentielles aux personnes qui consultent le site ou utilisent l'application. Ces mentions doivent faire apparaître l'identité du responsable de traitement, la finalité du traitement, le caractère obligatoire ou facultatif des données collectées, le ou les destinataires des informations, les transmissions de données vers des pays situés en dehors de l'Union Européenne, l'existence de droits des personnes concernées et notamment le droit de définir des directives quant au sort des données après sa mort. Ces mentions légales doivent également rappeler les conséquences en cas d'absence de réponse du responsable de traitement si une personne demande à faire appliquer ses droits. Bien évidemment, ces informations doivent être facilement consultables et compréhensibles par l'utilisateur.

Les cookies font partie des outils dont disposent les sites web pour tracer les actions de leurs utilisateurs et contribuer par un croisement de données à identifier une personne physique. De ce fait, ils deviennent donc sujets au RGPD et l'utilisateur d'un site web doit être averti de leur présence, donner son consentement préalablement à l'insertion de traceurs et avoir la possibilité d'accepter ou refuser les différents traitements associés.

C'EST QUOI UN COOKIE ?

Introduits par la société Netscape en 1995 avec la version 2.0 de son navigateur, les cookies offrent une solution aux programmeurs pour créer des données persistantes sur les postes clients. Les publicitaires les ont rapidement utilisés afin d'enregistrer les habitudes de consommation des individus.

Un cookie est déposé sur votre disque dur à la demande d'un serveur web par votre navigateur. L'objectif est de mettre en place une gestion de contexte afin de conserver des informations entre les différentes transactions effectuées par le client vers le serveur. À chaque requête vers un serveur web, votre navigateur vérifie qu'un cookie existe pour le domaine où réside la page demandée, pour le serveur où réside la page demandée ou encore pour la page demandée. Si l'une de ces conditions est vraie, le cookie est retourné au serveur web qui peut alors établir l'identité de la personne connectée.

Il est préférable d'appliquer un retour automatique au mode *Opt-out* et de laisser l'utilisateur configurer l'utilisation des cookies. Ceux-ci doivent avoir une durée de vie maximale de 13 mois. Notez également que ce qui est vrai pour les cookies, l'est également pour les nombreuses autres méthodes de traçage telles que les pixels invisibles ou encore la technique du *fingerprinting* (calcul d'un identifiant unique de la machine basée sur des éléments de sa configuration) **[10]**.

Toujours dans le domaine du traçage des individus, n'oubliez pas que des journaux d'activité tels que ceux d'un serveur web contiennent généralement des adresses IP et que celles-ci sont considérées comme étant des données personnelles. Au sein d'un organisme, le Code du travail précise qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. Il faut donc veiller à informer chaque salarié des finalités poursuivies, des destinataires des données, de son droit d'opposition pour motif légitime et de ses droits d'accès et de rectification.

3.4 Gérer et archiver des données

La gestion des données pose de nombreux problèmes aux informaticiens dans le cadre d'une application correcte du RGPD. La première difficulté porte sur le respect des droits des personnes.

La portabilité implique la possibilité d'extraire d'un système d'information l'intégralité des données à caractère personnel qu'un organisme a collecté sur une personne physique. Cela suppose donc de mettre en œuvre un traitement capable de retrouver ces données dans plusieurs sources de nature différentes (bases de données, fichiers plats, journaux de connexion, serveur de messagerie, etc.) et de les formater dans un ou plusieurs documents lisibles.

Le droit d'être exclus d'un traitement peut imposer des modifications complexes au code informatique des applications ainsi qu'aux bases de données exploitées. En effet, il faut être capable de distinguer au sein des données, celles pouvant être traitées et celles qui ne le doivent pas.

Enfin, le droit à l'oubli introduit également un certain nombre de problèmes techniques. Tout d'abord, il faut distinguer l'effacement du déréférencement. Ce dernier concerne principalement les moteurs de recherche et exercer ce droit permet à une personne physique de faire disparaître du résultat des recherches des données susceptibles de lui nuire. Ce droit n'implique pas la destruction des données, mais uniquement un marquage de celles-ci afin de les cacher.

Le droit à l'effacement est plus complexe en particulier si vous travaillez avec une base de données dans laquelle des relations sont définies entre les entités. Détruire des éléments peut rapidement mener à altérer l'intégrité structurelle de la base de données qui d'ailleurs, si elle a été correctement réalisée et utilise pleinement des contraintes d'intégrité, peut tout simplement rendre impossible la destruction de certaines données. Il faut donc appliquer le principe du *Privacy by Design* en prenant en compte le RGPD dès l'étape de conception d'une base de données. L'objectif est de ne pas se retrouver dans une impasse technique lorsque celle-ci sera en exploitation.

La conservation des données est également concernée par le RGPD. Vous avez vu précédemment qu'il

EXERCER VOTRE DROIT À LA PORTABILITÉ SUR FACEBOOK

Vous avez la possibilité d'expérimenter la portabilité des données sur le réseau social Facebook. Pour cela, sélectionnez l'option *Paramètres* et cliquez sur *Vos informations Facebook* puis sur *Téléchargez vos informations*. Vous accédez alors à une page permettant de choisir la période pour laquelle vous voulez obtenir vos données, le format d'extraction et les différentes catégories de données récupérables. Il ne vous reste plus qu'à cliquer sur le bouton *Créer un fichier*.

est obligatoire de définir une durée de conservation pour les données à caractère personnel et que cela doit être explicitement indiqué dans la fiche de traitement. Les informations doivent respecter une politique d'archivage découpée en trois grandes périodes. Pour leur utilisation courante, les données sont stockées en base active et sont donc accessibles à une ou plusieurs applications dans le cadre du traitement. Les données ne doivent être conservées en ligne ou en base active que pour la durée nécessaire à la finalité. Ensuite, lorsque les données ne sont plus concernées par l'exploitation courante, elles sont transférées dans des archives intermédiaires si elles présentent un intérêt administratif. Il est ainsi encore possible d'accéder aux données afin par exemple d'émettre un justificatif à la demande de la personne concernée. Enfin, si les données présentent un intérêt historique, scientifique ou statistique, elles rejoignent les archives définitives dans lesquelles elles sont anonymisées ou pseudonymisées. Dans le cas contraire, les données font l'objet d'une procédure d'effacement.

CONCLUSION

Vous voici au terme de cette présentation des principales caractéristiques du Règlement Général sur la Protection des Données. Celui-ci enrichit sur de nombreux points la loi Informatique et Libertés et renforce les pouvoirs de la CNIL. En avril 2019, lors de la présentation du rapport d'activité de la commission, sa présidente Marie-Laure Denis a annoncé la fin d'une période de tolérance à l'égard des entreprises qui contreviennent au RGPD. L'année 2018 a été celle du record de plaintes recueillies avec plus de 11077 plaintes (+32% par rapport à 2017) et pas moins de 1170 notifications de violations de données ont été signalées. Que l'on soit citoyen, informaticien dans le secteur public ou privé, responsable d'une association, il est donc essentiel de comprendre et d'appliquer le RGPD afin de mesurer avec précision la responsabilité et l'impact du traitement de données à caractère personnel. ■

RÉFÉRENCES

[1] Edward Snowden : https://fr.wikipedia.org/wiki/Edward_Snowden

[2] Nest Secure, le micro caché et la confiance : https://www.minimachines.net/actu/nest-secure-75835

[3] Amazon Workers Are Listening to What You Tell Alexa : https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

[4] Le logiciel PIA de la CNIL : https://www.cnil.fr/fr/analyse-dimpact-la-version-20-de-loutil-pia-est-disponible.

[5] La protection des données dans le monde : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

[6] Transférer des données hors de l'UE : https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue

[7] Exemple de registre : https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

[8] Le site de l'ANSSI : https://www.ssi.gouv.fr

[9] Exemples de mentions d'information : https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

[10] Le fingerprinting : https://www.inria.fr/centre/lille/actualites/souriez-vous-etes-traque

POUR ALLER PLUS LOIN

- **Le Règlement (UE) 2016/679 :** https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- **Le site de la CNIL :** https://www.cnil.fr
- **Rapport d'activité de la CNIL :** https://www.cnil.fr/fr/presentation-du-rapport-dactivite-2018-et-des-enjeux-2019-de-la-cnil
- **L'atelier RGPD :** https://atelier-rgpd.cnil.fr/
- **Le MOOC sur la sécurité de l'ANSSI :** https://secnumacademie.gouv.fr/

L'OPEN SOURCE AU CŒUR DU PARTAGE DE LOW-TECHNOLOGIES : À LA DÉCOUVERTE DU LOW TECH LAB

MARIER OPEN SOURCE, BASSES OU « LOW » TECHNOLOGIES ET DÉVELOPPEMENT DURABLE, TEL EST L'UN DES OBJECTIFS SUIVIS PAR LE LOW TECH LAB, UN COLLECTIF ASSOCIATIF QUI SE VEUT PROMOUVOIR LES SOLUTIONS UTILES ET DURABLES. PIERRE-ALAIN, L'UN DES PORTEURS DE CE COLLECTIF A BIEN VOULU NOUS ÉCLAIRER DAVANTAGE SUR LE SUJET ET RÉPONDRE À NOS QUESTIONS.

Site du projet : **https://lowtechlab.org/wiki/Accueil**

L'équipe lors du Low-tech Tour effectué en 2017.

Linux Pratique :

Pouvez-vous vous présenter et nous parler de votre parcours ?

Je m'appelle Pierre-Alain, j'ai 29 ans, je suis passionné par les techniques et bonnes pratiques permettant un avenir durable pour la planète et l'homme. J'ai une formation d'ingénieur généraliste et j'ai rejoint le Low-tech Lab à ses tous débuts en 2012 au Bangladesh pour mon stage de fin d'études.

Ma première mission a été de concevoir des machines pour produire un tissu pour composite en fibre de jute en s'adaptant aux machines traditionnelles bengali puis nous avons construit Gold Of Bengal le premier voilier en fibres naturelles sur lequel Corentin de Chatelperron, le fondateur de l'association, est parti en test à la fois de notre matériau et de l'autonomie grâce à des systèmes simples : les Low-tech.

Suite à cette expérience, qui ne fut pas une grande réussite technique, mais riche en apprentissage, nous nous sommes rendu compte du potentiel de ces low-tech et de l'importance de pouvoir les mettre en lumière et connecter acteurs et bénéficiaires. Nous avons donc lancé l'expédition Nomade des Mers en parallèle d'un wiki en ligne de documentation open source en 2014. J'avais principalement une casquette technique de veille, de prise de contact avec des experts de préparation du bateau puis de rencontre avec les inventeurs au travers le monde sur le bateau.

À mon retour en France, nous nous sommes questionnés sur la manière dont les low-tech pouvaient également s'adapter dans notre contexte français/occidental. Nous avons donc réalisé le Low-tech Tour entre 2017 et 2018 qui nous a permis, en parallèle du Nomade des Mers, de documenter 12 low-tech adaptées à l'habitat français, de l'éolienne au chauffage solaire.

Je suis aujourd'hui principalement sur le projet d'habitat low-tech, une maison prototype dans laquelle on vise l'autonomie grâce aux low-tech tout en démontrant qu'elles sont pertinentes d'un point de vue économique, écologique et ergonomique.

Linux Pratique :

Comment peut-on définir le « low tech » ?

Au Low-tech Lab, nous appelons low-tech les objets, les systèmes, les techniques, les services, les savoir-faire, les pratiques, les comportements et même les courants de pensée qui s'articulent autour de trois principes :

1) La low-tech est avant tout utile : elle répond à des besoins essentiels tels que l'accès à l'eau, l'alimentation, l'énergie, l'habitat ou l'hygiène. Par extension, elle peut concerner les domaines de la santé, des transports, des matériaux de construction et de fabrication, de la gestion des déchets, de l'agriculture ou encore de l'éducation. En revenant à l'essentiel, elle redonne du sens à l'action, et elle rend possible des modes de vie sains et épanouissants.

> Nous avons lancé l'expédition Nomade des Mers en parallèle d'un wiki en ligne de documentation open source en 2014.

2) La low-tech est ensuite intrinsèquement durable. Elle est durable au sens où elle est robuste, modulaire, réparable, fonctionnelle. etc. Elle est également durable d'un point de vue écologique puisqu'elle vise la sobriété : l'économie d'énergie et l'efficacité énergétique, autant que l'économie et l'emploi optimal de matière. Concrètement, l'approche low-tech s'intéresse en priorité aux sources d'énergies et de ressources renouvelables et disponibles localement ; elle se base sur une connaissance poussée des écosystèmes, s'inspire de la nature et cherche à faire avec elle, notamment en respectant les rythmes de régénération ou de dégradation, en favorisant l'emploi de matières peu transformées et non toxiques, la valorisation de déchets, etc. Elle est finalement durable à une échelle sociétale puisqu'en pensant des solutions, des activités et des connaissances relocalisées, on diminue autant l'empreinte environnementale

que l'empreinte sociale de celles-ci, et on peut sortir de logique d'exploitations.

3) La low-tech est enfin accessible au plus grand nombre. D'un point de vue économique : en étant simple, optimisée, robuste, fabriquée et réparée localement elle est souvent moins coûteuse et permet ainsi à chacun de répondre plus durablement à ses besoins essentiels. Mais également accessible en termes de connaissances : l'approche low-tech permet de démocratiser la technique, non pas au sens de plus de technologies pour tout le monde mais au sens d'ouvrir les savoir et de libérer la créativité, l'ingéniosité de chacun et le pouvoir d'agir collectif, tout en les orientant vers l'humain au sein de son environnement. Elle favorise donc une plus grande autonomie des populations à tous les niveaux, ainsi qu'une meilleure répartition de la valeur ou du travail.

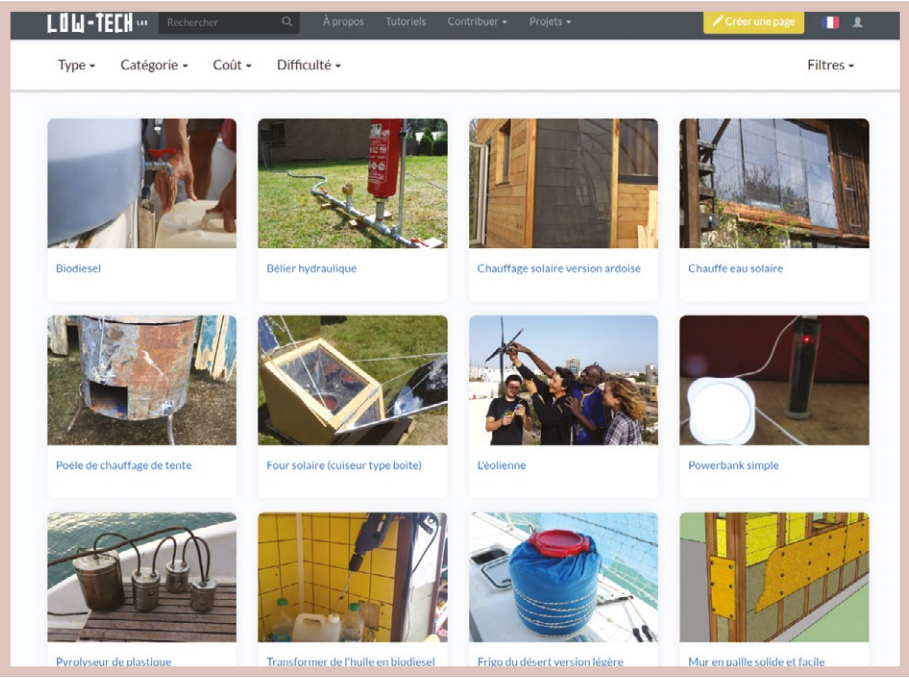
> « L'open source est l'un des piliers de notre vision : le partage libre des connaissances autour des low-tech est essentiel d'une part dans une optique d'optimisation.

Linux Pratique :

Qu'est-ce que le Low Tech Lab ? Quelles sont vos missions ?

Depuis 2012, nous faisons le constat que des solutions low-tech existent déjà un peu partout, qu'elles émergent presque spontanément de la société civile. Nous sommes convaincus que si elles étaient plus largement connues, adaptées, répliquées, elles permettraient de lutter localement et efficacement contre les maux du XXIème siècle. En offrant la possibilité de subvenir sainement à ses besoins, au sein de communautés résilientes et d'écosystèmes régénérés, la low-tech s'attaque à la fois à la pauvreté, au réchauffement climatique, aux inégalités ou à la pollution, par ailleurs tous profondément liés.

Alors aujourd'hui nous œuvrons au quotidien pour donner à chacun l'envie et les moyens de vivre mieux avec moins. Nous voulons être les ambassadeurs de ces modes de vie, de consommation ou de production plus sobres, plus collaboratifs et plus épanouissants, qui fédèrent avant tout par le sens et l'éthique qu'ils redonnent au quotidien. Pour cela, nous portons plusieurs projets d'expérimentation terrain, nous dénichons ces solutions en France et partout dans le monde, nous les testons en conditions réelles pour mieux les comprendre, et nous nous attachons à démontrer la pertinence de cette approche dans différents contextes (des pays occidentaux aux pays émergents de la ceinture tropicale en passant par les camps de réfugiés au Nord comme au Sud) ainsi que dans différents domaines d'application (premières nécessités, habitat,



Les nombreux tutoriels tirant parti des low-technologies mis à disposition de tous sur le site du projet.

ACTUELLEMENT DISPONIBLE

HACKABLE N°30 !

NOUVELLE FORMULE !

NOUVELLE FORMULE : + RUBRIQUE « SÉCURITÉ » + RUBRIQUE « ROBOTIQUE » + 32 PAGES
HACKABLE
MAGAZINE
DÉMONTEZ | COMPRENEZ | ADAPTEZ | PARTAGEZ
N° 30
JUILLET / AOÛT / SEPTEMBRE 2019
NOUVELLE RUBRIQUE
SÉCURITÉ / NFC
Éprouvez la sécurité de vos tags RFID avec le Proxmark 3
NOUVELLE RUBRIQUE
ROBOTIQUE / LEGO
Contrôlez vos Lego PoweredUp avec votre Raspberry Pi
RADIO / SDR
Décodez les messages d'un horrible collier de dressage canin
ARDUINO / USB
Ajoutez à Linux des leds USB pilotables via /sys/class/leds
Arduino / capteurs / mesure :
Détectez la RADIOACTIVITÉ
• Connaître les principes
• Choisir le matériel
• Créer son détecteur
DOMOTIQUE / TEMPS
Créer un calculateur de départ différé pour votre lave linge
AFFICHEUR / TWITTER
Comptez et affichez vos followers Twitter avec un ESP8266

NE LE MANQUEZ PAS

CHEZ VOTRE MARCHAND DE JOURNAUX ET SUR :

https://www.ed-diamond.com

mobilité). Nous documentons, diffusons et transmettons, en ligne et en open source, les fruits de ces expérimentations pour sensibiliser tout un chacun, mais surtout pour qu'il ou elle puisse accéder librement à ces outils, ces techniques et ces modes de vie, se les approprier et les adapter à son propre contexte : ressources naturelles et gisements de déchets locaux, compétences et savoir-faire disponibles, croyances et habitudes culturelles.

> La première manière de participer est d'agir soi-même dans son quotidien pour tendre vers plus de sobriété : requestionner ses besoins !

Linux Pratique :

L'open source a une grande place dans vos initiatives ?

L'open source est l'un des piliers de notre vision : le partage libre des connaissances autour des low-tech est essentiel d'une part dans une optique d'optimisation. Chaque personne avec ses compétences ou son usage peut apporter sa pierre pour optimiser et adapter des principes techniques à son contexte. D'autre part, pour la diffusion, l'open source permet à chacun localement de s'approprier la technique, de fabriquer des low-tech, pourquoi pas de créer une économie locale si celle-ci reste dans un cadre de valeurs cohérentes avec la philosophie low-tech.

Le projet d'habitat low-tech sur lequel travaille notamment Pierre-Alain actuellement.

Linux Pratique :

Quels projets menez-vous actuellement ?

Je mène en ce moment le projet d'habitat low-tech : une maison prototype qui rassemble un best-of de low-tech adaptées au contexte français. Nous vivons dans cette maison avec pour objectif d'atteindre l'autonomie énergétique en eau tout en produisant le moins de déchets possible. Nous y faisons de nombreuses mesures afin de démontrer la pertinence économique, écologique et ergonomique de ces systèmes.

Nous réalisons d'ailleurs une série sur la vie dans cet habitat, diffusée en ce moment sur Internet.

Linux Pratique :

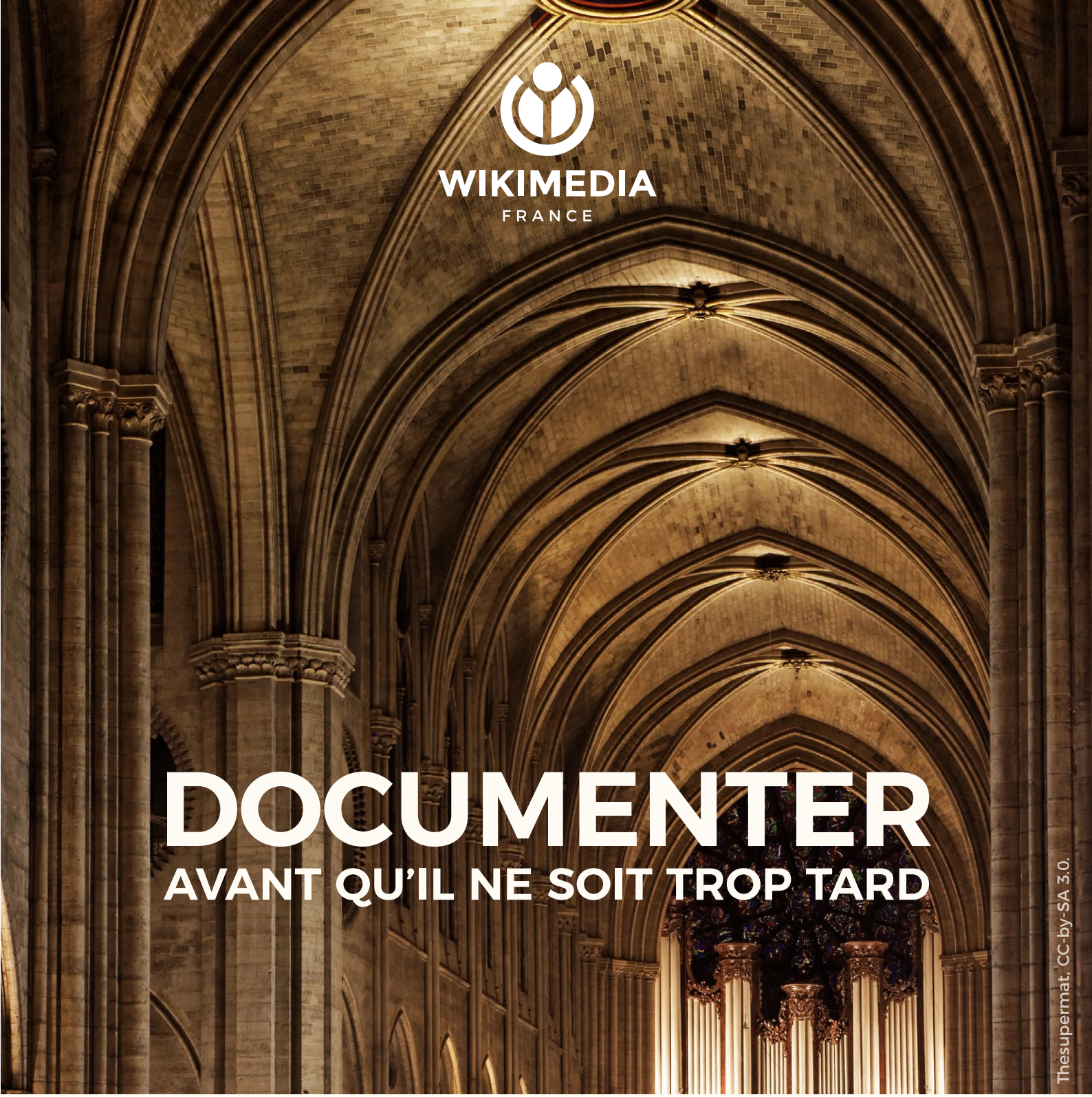
Existe-t-il d'autres initiatives telles que la vôtre à travers le monde ?

Beaucoup de personnes et d'organismes sont sur le sujet des low-tech, chacun avec leur spécificité. Par exemple Practical Action, en Grande-Bretagne, est une ONG qui œuvre depuis les années 60 pour diffuser les low-tech.

Linux Pratique :

Comment peut-on participer ?

La première manière de participer est d'agir soi-même dans son quotidien pour tendre vers plus de sobriété : requestionner ses besoins ! Après, toutes les aides sont utiles, du retour d'usagers à des compétences techniques en passant par de la traduction de tutoriels par exemple. Rendez-vous sur https://lowtechlab.org/. ■



WIKIPEDIA
L'encyclopédie Libre

WIKIMEDIA COMMONS

WIKISOURCE

WIKIDATA

Partagez vos connaissances de la cathédrale librement afin que les générations futures puissent témoigner de la longue histoire de Notre-Dame de Paris.

Plus d'informations sur www.wikimedia.fr

FIRST EUROPEAN
FREE & OPEN
SOURCE EVENT

opensourcesummit.paris

#OSSPARIS19

PARIS REGION SMART WEEKS

La FRENCH TECH

PARIS OPEN SOURCE SUMMIT

5e ÉDITION

10 & 11 DECEMBRE 2019

Show and Congress
Dock Pullman

Pour toute demande d'informations complémentaires :
Email : cjardon@weyou-group.com – Tel : 01 41 18 60 52

un événement

Systematic Paris Region Digital Ecosystem

weyou Group

en partenariat avec

îledeFrance

CNLL

partenaire média

LINUX PRATIQUE

co-organisateurs

alter way

BlueMind Messagerie & espaces collaboratifs

Inria

SensioLabs Créateur de Symfony

Smile OPEN SOURCE SOLUTIONS

Vorteks make IT work, make IT free